HP MSM7xx Controllers CLI

Reference Guide

HP MSM7xx Controllers

CLI Reference Guide

© Copyright 2011 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard.

Publication Number
5998-1432
December 2011

Applicable Products

See *Products covered on page 1-2*.

Trademark Credits

Windows NT®, Windows®, and MS Windows® are US registered trademarks of Microsoft Corporation.

sFlow

Disclaimer

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Hewlett-Packard Company
8000 Foothills Boulevard
Roseville, California 95747
www.hp.com/networking

Contents

1 Introduction

About this guide 1-2
Products covered 1-2
Important terms 1-2
Typographical conventions 1-2
Command syntax 1-2
Management tool 1-3
New in this release 1-4
HP support 1-4
Before contacting support 1-4
Online documentation 1-5
Configuring CLI support 1-5
Secure shell access 1-6
Authentication 1-6
Serial port access 1-7
Starting a CLI session on the serial port 1-7
Entering strings 1-8
Context hierarchy 1-9
Sample CLl sessions 1-10
Example 1 1-10
Example 2 1-11
Example 3 1-11
File transfer 1-12
A. The controller gets the file using a URL 1-12
B. Send a file to the controller 1-12

2 CLI commands

View context 2-3
arping 2-3
enable 2-3
nslookup 2-3
ping 2-3
ps 2-3
quit 2-3
show license 2-4
show logging filtered 2-4
top 2-4
traceroute 2-4

Enable context 2-5
reboot device 2-5
show certificate 2-5
show certificate binding 2-5
iperf 2-5
ping 2-5
arping 2-6
arp 2-6
end 2-6
quit 2-6
rcapture 2-6
show arp 2-6
show bridge 2-7
show bridge forwarding 2-7
show dns cache 2-7
show interfaces 2-7
show ip 2-7
show ip route 2-7
show system info 2-7
show vsc overview 2-7
show controlled-aps wireless clients 2-8
disassociate controlled-ap wireless client _ 2-8
show ip dhcp database 2-8
show satellites 2-8
show web content 2-8
show client log 2-8

show radius statistics 2-8
show radius users 2-8
show users 2-9
show discrete pin 2-9
config 2-9
show all config 2-9
controlled network 2-9
show controlled network config 2-9

Config context 2-10
vlan 2-10
New interface 2-10
dhcp public ip default lease period 2-10
dhcp public ip subnet 2-10
certificate 2-10
certificate binding 2-10
certificate revocation 2-11
end 2-11
factory settings 2-11
network-profile 2-11
reboot device 2-11
show certificate 2-11
show certificate binding 2-11
show config factory 2-12
show network-profiles 2-12
show tech 2-12
interface ethernet 2-12
interface ip 2-12
interface pptp client-default 2-12
interface gre 2-12
New show lacp 2-13
New show mac-address 2-13
New show mac-address count 2-13
New show trunks 2-13
New show vlans 2-13
virtual ap 2-13
cap-switch to 2-13
show subscription plan 2-14
subscription plan 2-14
mac list 2-14

show mac list 2-14
ipsec policy 2-14
admin local authentication 2-14
admin radius authentication 2-15
admin radius authentication server 2-15
ip http port 2-15
ip https port 2-15
snmp-server trap certificate-expired 2-15
snmp-server trap certificate-expires-soon 2-16
snmp-server trap web-fail 2-16
snmp-server trap web-login 2-16
snmp-server trap web-logout 2-16
username 2-16
web admin kickout 2-17
web allow 2-17
web access internet-port 2-17
web access lan-port 2-17
web access interface vlan 2-17
web access interface gre 2-18
web access vpn 2-18
web access lan 2-18
dhcp mode 2-18
enable console password reset 2-18
console authentication 2-18
dhcp server 2-19
dhcp server default domain name 2-19
dhcp server default lease period 2-19
dhcp server default permanent lease period 2-19
dhcp server controller 2-19
dhcp server controller discovery 2-19
dhcp server logout html user 2-20
dhcp server access centralized clients 2-20
dhcp server access lan 2-20
dhcp relay 2-20
dhcp relay circuit id 2-20
dhcp relay remote id 2-21
dhcp relay access centralized clients 2-21
dhcp relay access lan 2-21
New dhcp relay access access network 2-21

dhcp relay extend internet port 2-21
New dhcp relay extend internet network 2-22
clock 2-22
clock auto adjust dst 2-22
clock timezone 2-22
clock use custom dst rules 2-22
ntp protocol 2-23
ntp server 2-23
clock custom dst begins 2-23
clock custom dst begins format 2-23
clock custom dst ends 2-24
clock custom dst ends format 2-24
ntp server 2-24
ntp server failure trap 2-24
config-update automatic 2-25
config-update operation 2-25
config-update start 2-25
config-update time 2-25
config-update uri 2-25
config-update weekday 2-25
snmp-server trap config-change 2-26
snmp-server trap config-update 2-26
logging destination 2-26
snmp-server trap syslog-severity 2-26
snmp-server 2-26
snmp-server allow 2-27
snmp-server chassis-id 2-27
snmp-server contact 2-27
snmp-server heartbeat period 2-27
snmp-server location 2-27
snmp-server port 2-28
snmp-server readonly 2-28
snmp-server readwrite 2-28
snmp-server trap 2-28
snmp-server trap community 2-28
snmp-server trap destination 2-29
snmp-server trap heartbeat 2-29
snmp-server trap link-state 2-29
snmp-server trap snmp-authentication 2-29

snmp-server version 1 2-29
snmp-server version 2c 2-30
snmp-server version 3 2-30
snmp-server access interface vlan 2-30
snmp-server access interface gre 2-30
snmp-server access port-1 2-30
snmp-server access port-2 2-31
snmp-server access vpn 2-31
snmp-server trap device-authorization-failure 2-31
snmp-server trap device-configuration-failure 2-31
snmp-server trap device-firmware-failure 2-31
snmp-server trap device-security-failure 2-32
snmp-server trap device-state-change 2-32
snmp-server trap new-satellite-detected 2-32
snmp-server trap satellite-unreachable 2-32
snmp-server trap service-controller-state 2-32
snmp-server access lan 2-33
snmp-server user 2-33
snmp-server notification receiver 2-33
soap-server 2-33
soap-server access interface vlan 2-33
soap-server allow 2-34
soap-server http authentication 2-34
soap-server http authentication password 2-34
soap-server http authentication username 2-34
soap-server port 2-34
soap-server ssl 2-34
soap-server ssl with client certificate 2-35
soap-server access interface gre 2-35
soap-server access port-1 2-35
soap-server access port-2 2-35
soap-server access lan 2-35
soap-server access vpn 2-36
snmp-server trap vpn-connection 2-36
snmp-server trap syslog-matches 2-36
snmp-server trap syslog-matches regex 2-36
snmp-server trap syslog-severity level 2-36
snmp-server trap network-trace 2-36
firmware-update automatic 2-37

firmware-update start 2-37
firmware-update time 2-37
firmware-update uri 2-37
firmware-update weekday 2-38
snmp-server trap firmware-update 2-38
ip name-server 2-38
ip name-server cache 2-38
ip name-server dynamic 2-38
ip name-server interception 2-39
ip name-server switch-on-servfail 2-39
ip name-server switch-over 2-39
ip name-server logout-info 2-39
access controller shared secret 2-39
radius-server profile 2-40
ip-qos profile 2-40
access controller 2-40
certificate ipsec ca 2-40
certificate ipsec local 2-40
certificate ipsec revocation 2-41
certificate ssl 2-41
session profile default 2-41
session profile 2-41
show session profile 2-41
remote configuration 2-41
lldp config 2-42
lldp dynamic-name 2-42
lldp dynamic-name refresh-time 2-42
lldp dynamic-name user-string 2-42
lldp fast-start-count 2-42
lldp holdtime-multiplier 2-43
lldp med-location civic-address-element 2-43
lldp med-location elin-addr 2-43
lldp refresh-interval 2-43
lldp run 2-43
show lldp config 2-43
show lldp info local-device 2-43
show lldp info remote-device 2-44
show lldp stats 2-44
discovery protocol 2-44

discovery protocol device-id 2-44
service controller ap authentication credentials 2-44
service controller ap authentication enable 2-44
service controller ap authentication file 2-45
service controller ap authentication radius-server 2-45
service controller ap authentication refresh-rate 2-45
service controller ap authentication source file 2-45
service controller ap authentication source local 2-45
service controller ap authentication source radius 2-45
service controller discovery 2-46
service controller primary 2-46
service controller primary ip addr 2-46
service controller priority 2-46
service controller discovery interface internet-port 2-46
service controller discovery interface lan-port 2-46
New service controller discovery interface 2-47
service controller provisioning 2-47
bandwidth control internet-port 2-47
bandwidth control internet-port high 2-47
bandwidth control internet-port low 2-47
bandwidth control internet-port max-rate 2-47
bandwidth control internet-port normal 2-48
bandwidth control internet-port very-high 2-48
New bandwidth control 2-49
New bandwidth control high 2-49
New bandwidth control low 2-49
New bandwidth control max-rate 2-49
New bandwidth control normal 2-50
New bandwidth control very-high 2-50
ip route gateway 2-50
firewall mode 2-51
show user profiles 2-51
show user profiles details 2-51
user profile 2-51
renew user profile subscription 2-51
New dot1x radius accounting start delay 2-51
dot1x reauth 2-52
dot1x reauth period 2-52
dot1x reauth terminate 2-52

dot1x supplicant timeout 2-52
dynamic key 2-52
dynamic key interval 2-53
key chain 2-53
config-version 2-53
radius-server accounting session 2-53
radius-server client 2-53
radius-server local eap-peap 2-53
radius-server local eap-tls 2-54
radius-server local eap-ttls 2-54
radius-server local pap 2-54
radius-server ssid detection nas-id 2-54
show radius-server 2-54
active-directory check attribute 2-54
active-directory check user access 2-55
active-directory device name 2-55
active-directory domain 2-55
active-directory domain netbios name 2-55
active-directory group 2-55
active-directory group order 2-55
active-directory join 2-56
show active-directory 2-56
show active-directory group 2-56
radius-server client 2-56
user tracking 2-56
user tracking destination 2-56
user tracking filter 2-56
user tracking port 2-57
persistent user information 2-57
persistent user information period 2-57
client data tunnel security 2-57
igmp proxy 2-57
igmp proxy downstream interface 2-57
igmp proxy upstream interface 2-57
rf-id aeroscout 2-58
sflow 2-58
show sflow agent 2-58
show sflow controller stats 2-58
show sflow device stats 2-58

sflow destination 80211 2-58
show sflow destination 2-58
show sflow sampling-polling 2-59
sflow sampling 2-59
sflow polling 2-59
sflow interface 2-59
mac lockout entry 2-59
show mac lockout 2-59
New team communication ip address 2-59
New team communication vlan 2-60
team management address 2-60
team manager 2-60
New team name 2-60
teaming 2-60
New team communication interface 2-60
New team communication interface 2-60
New team communication vlan 2-61
team management interface 2-61
team management interface vlan 2-61

Access Controller context 2-62
end 2-62
ads presentation 2-62
ads presentation interval 2-62
station free access 2-62
station http proxy html authentication only support 2-62
station http proxy support 2-63
station idle detection 2-63
system accounting 2-63
remember delay 2-63
remember html users 2-64
worldpay installation id 2-64
worldpay payment response password 2-64
worldpay payment url 2-64
authorize_net installation id 2-64
authorize_net payment url 2-64
authorize_net transaction key 2-64
show paypal 2-65
paypal api-url 2-65
paypal operation-mode 2-65

paypal password 2-65
paypal signature 2-65
paypal user-id 2-65
ads presentation with frameset 2-65
authentication http 2-66
authentication https 2-66
local welcome-page 2-66
noc access internet 2-66
noc access vpn 2-66
noc allow 2-66
noc authentication 2-67
secure login 2-67
sslv2 authentication 2-67
user-agent block 2-67
user-agent filtering 2-67
noc access interface vlan 2-68
noc access interface gre 2-68
ipass id 2-68
ipass name 2-68
wispr abort login url 2-68
wispr login url 2-69
wispr logoff url 2-69
access-list 2-69
use access-list 2-70
use access-list unauth 2-70
config file 2-70
http proxy upstream 2-71
https ssl certificate 2-71
mac-address 2-71
fail page 2-71
goodbye url 2-71
ipass login url 2-72
login error url 2-72
login page 2-72
login url 2-72
logo 2-72
messages 2-73
noc ssl ca-certificate 2-73
noc ssl certificate 2-73

session page 2-73
transport page 2-73
welcome url 2-74
notify user location changes 2-74

Default user session profile context 2-75
accounting interim update 2-75
idle timeout 2-75
maximum input octets 2-75
maximum input packets 2-75
maximum output octets 2-76
maximum output packets 2-76
maximum total octets 2-76
maximum total packets 2-76
nat one-to-one 2-76
session timeout 2-77
smtp redirection setup 2-77
public ip subnet 2-77
end 2-77
smtp redirection 2-78

Session profile context 2-79
end 2-79
access controlled 2-79
access list 2-79
accounting interim update 2-79
arp polling interval 2-80
arp polling max count 2-80
bandwidth level 2-80
egress vlan 2-80
idle timeout 2-81
intercept traffic 2-81
max input rate 2-81
max output rate 2-81
nat one-to-one 2-82
session profile 2-82
smtp redirection setup 2-82
termination action 2-83
user defined attribute 2-83
public ip subnet 2-83

User account context 2-85
end 2-85
access controlled 2-85
access-controlled profile 2-85
access-controlled virtual ap 2-85
active 2-86
chargeable user identity 2-86
control method 2-86
egress vlan 2-86
end time 2-86
idle timeout 2-86
max user sessions 2-87
password 2-87
regular profile 2-87
regular virtual ap 2-87
session timeout 2-87
subscription plan 2-88
username 2-88

Internet port interface context 2-89
end 2-89
duplex 2-89
speed 2-89
interface vlan 2-89
ipsec vlan interface 2-90

LAN port interface context 2-91
end 2-91
duplex 2-91
speed 2-91
interface vlan 2-91
ipsec vlan interface 2-92

WAN IP interface context 2-93
pppoe client user 2-93
New tagged 2-93
New untagged 2-93
ip address mode 2-93
ip address 2-94
ip nat 2-94
nat limit port range 2-94

nat limit port range size 2-94
ip address dhcp client-id 2-94
end 2-95
pppoe auto-reconnect 2-95
pppoe mru 2-95
pppoe mtu 2-95
pppoe unnumbered 2-95
ip nat outside source static 2-96
ip address alternate 2-96

LAN IP interface context 2-97
end 2-97
ip address 2-97
ip address management 2-97
New tagged 2-97
New untagged 2-97

Public access RADIUS attributes context 2-98
end 2-98
active 2-98
credentials 2-98
interval 2-98
radius server profile 2-98

Virtual AP context 2-99
virtual ap name 2-99
access control 2-99
force centralize data 2-99
ingress interface 2-100
egress unauthenticated 2-100
guest-mode 2-100
max-association 2-100
ssid name 2-101
encryption key 1 2-101
encryption key format 2-101
transmit key 2-101
authentication server access controller 2-102
authentication server accounting 2-102
authentication server accounting radius profile 2-102
authentication server radius 2-102
dot1x authentication 2-102

wpa-psk 2-102
authentication server request radius cui 2-103
dot1x session page 2-103
New wpa terminate controller 2-103
wireless filters 2-103
wireless filters mac 2-103
wireless filters rule input 2-104
wireless filters rule output 2-104
wireless filters type 2-104
mac-filters local 2-105
mac-filters 2-106
mac-filters mode 2-106
mac authentication accounting 2-106
mac authentication accounting radius profile 2-106
mac authentication radius profile 2-106
mac authentication remote 2-107
mac authentication request radius cui 2-107
mac authentication local 2-107
mac authentication 2-107
html authentication 2-107
html authentication accounting 2-108
html authentication accounting radius profile 2-108
html authentication active-directory 2-108
html authentication local 2-108
html authentication radius 2-108
html authentication radius profile 2-108
html authentication request radius cui 2-109
html authentication timeout 2-109
active 2-109
band steering 2-109
beacon dtim count 2-109
beacon transmit power 2-110
broadcast filter 2-110
data rate 2-110
public forwarding 2-110
access lan stations 2-110
fast authentication 2-110
layer3 mobility 2-111
layer3 mobility hns fallback method 2-111

layer3 mobility hns method 2-111
add ip-qos profile 2-111
delete ip-qos profile all 2-111
delete ip-qos profile 2-111
qos 2-112
upstream diffserv tagging 2-113
wmm advertising 2-113
html redirection 2-113
local nas id 2-113
bandwidth 2-113
bandwidth default rates 2-113
bandwidth default rates maximum 2-114
radius accounting realms 2-114
radius authentication realms 2-114
identify stations by ip only 2-114
location-aware group 2-114
location-aware called-station-id content 2-115
dhcp relay 2-115
dhcp relay active 2-115
dhcp relay circuit id 2-115
dhcp relay remote id 2-115
dhcp relay subnet 2-115
dhcp server 2-116
dhcp server dns 2-116
dhcp server gateway 2-116
dhcp server range 2-116
dhcp server subnet 2-116
radius-framed-protocol-attribute 2-116
end 2-117
security 2-117

Interface context 2-118
New duplex-mode 2-118
New end 2-118
New flow-control 2-118
New flow-control auto-negotiation 2-118
New speed 2-118
New trunk group 2-118
New trunk type 2-119

VLAN interface context 2-120
end 2-120
ip address 2-120
ip address mode 2-120
New tagged 2-120
New untagged 2-120
ip default-gateway 2-121
ip nat 2-121

RADIUS profiles context 2-122
end 2-122
radius-server accounting port 2-122
radius-server alternate hosts 2-122
radius-server authentication method 2-122
radius-server authentication port 2-122
radius-server deadtime 2-123
radius-server host 2-123
radius-server key 2 2-123
radius-server message-authenticator 2-123
radius-server name 2-123
radius-server nasid 2-124
radius-server timeout 2-124
radius-server timeout 2-124
radius-server force-nas-port-to-vlanid 2-124
radius-server realm 2-124
radius-server realm name 2-124

IP QOS context 2-125
end 2-125
end-port 2-125
priority 2-125
profile name 2-125
protocol 2-125
start-port 2-125

DHCP server context 2-127
end 2-127
active 2-127
gateway 2-127
range 2-127
permanent leases 2-127

GRE interface context 2-128
end force 2-128
gre name 2-128
ip address 2-128
peer ip address 2-128
remote ip address 2-128

IPsec context 2-129
end 2-129
active 2-129
authentication 2-129
cipher 2-129
dns domain 2-129
dns server 2-129
incoming nat 2-130
incoming traffic network 2-130
interface 2-130
local id 2-130
mode 2-130
outgoing traffic network 2-130
peer id 2-130
peer ip address 2-131
perfect forward secrecy 2-131
preshared key 2-131

Syslog context 2-132
active 2-132
logging facility 2-132
logging host 2-132
logging prefix 2-132
name 2-132
logging source 2-133
end 2-133
level 2-133
level 2-133
matches 2-133
message 2-134
message 2-134
process 2-134
process 2-134

PPTP client interface 2-135
active 2-135
pptp client credentials 2-135
pptp client domain name 2-135
pptp client server address 2-135
end 2-135
ip nat 2-135
pptp client auto route discovery 2-136
pptp client lcp echo 2-136

Keychain context 2-137
end 2-137
key 2-137
key chain name 2-137

Keys context 2-138
end 2-138
key-string 2-138

Subscription plan context 2-139
end 2-139
daily restriction 2-139
end time 2-139
initial login time allocation 2-139
online time limit 2-140
online time limit 2-140
start time 2-140
subscription plan name 2-140
public ip reservation 2-140
public ip subnet 2-140

SNMP user context 2-142
access level 2-142
end 2-142
password 2-142
security 2-142
user name 2-142

SNMP notification receiver context 2-143
community 2-143
end 2-143
port 2-143

receiver 2-143
user 2-143
version 2-143

Active Directory Group context 2-144
end 2-144
access controlled 2-144
access-controlled profile 2-144
access-controlled virtual ap 2-144
active 2-145
active-directory group name 2-145
egress vlan 2-145
regular profile 2-145
regular virtual ap 2-145

Controlled APs context 2-147
end 2-147
execute action 2-147
execute system action 2-147
show config factory 2-147
ap group 2-147
ap name 2-147
config 2-147
contact 2-148
location 2-148
product type 2-148
product type 2-148

Controlled APs group context 2-149
execute action 2-149
show config factory 2-149
end 2-149
config 2-149
group name 2-149
virtual ap binding 2-149

Controlled APs base group context 2-150
execute action 2-150
show config factory 2-150
config 2-150
end 2-150

Controlled APs network configuration context 2-151
end 2-151
interface wireless 2-151
local mesh group 2-151
local mesh provisioning group 2-151
provisioning connectivity 2-151
provisioning discovery 2-151
radius profile 2-151
show tech 2-152
switch port 2-152
syslog 2-152
inherit vlan port2 2-152
vlan port2 2-152
vlan port2 id 2-152
inherit country code 2-152
world-mode dot11 country code 2-153
New inherit ipv6 ra conversion 2-153
New ipv6 ra conversion 2-153
New show ipv6 ra conversion 2-153
sensor server name 2-153
sensor server id 2-154
sensor discovery mode 2-154
sensor network detector 2-154
inherit sensor 2-154
dynamic key 2-155
dynamic key interval 2-155
dot1x reauth 2-155
dot1x reauth period 2-155
dot1x reauth terminate 2-155
dot1x supplicant timeout 2-156
inherit 8021x 2-156
bridge protocol ieee 2-156
inherit untagged stp 2-156
bridge protocol ieee vlan 2-156
inherit vlan stp 2-157
inherit local mesh qos 2-157
local mesh ip qos profile 2-157
local mesh qos mechanism 2-157
enable vsc services 2-157

inherit service availability 2-157
inherit l3subnets 2-158
l3subnet 2-158
inherit switch port _ 2-158
inherit switch ports 2-158
inherit lldp-app-profile 2-158
lldp app-profile 2-159
lldp app-profile 2-159
lldp app-profile 2-159
lldp app-profile 2-159
inherit lldp-general 2-159
lldp dynamic-name 2-159
lldp fast-start-count 2-160
lldp holdtime-multiplier 2-160
lldp local-mesh 2-160
lldp med-location civic-address-element 2-160
lldp med-location elin-addr 2-160
lldp refresh-interval 2-160
lldp run 2-161

Controlled APs VSC binding context 2-162
dual radio binding 2-162
egress vlan 2-162
egress vlan 2-162
end 2-162
location aware 2-162

Syslog context 2-163
message 2-163
message 2-163
process 2-163
process 2-163
level 2-163
level 2-164
matches 2-164
end 2-164
inherit 2-164

Provisioning connectivity context 2-165
end 2-165
inherit 2-165

interface 2-165
interface provisioning 2-165
ip assignation 2-165
vlan 2-166
vlan 2-166
static ip 2-166
provisioning local mesh group 2-166
provisioning local mesh key 2-166
provisioning local mesh port 2-166
provisioning local mesh security 2-166
provisioning local mesh security 2-167
provisioning local mesh type 2-167
country code 2-167
anonymous identity 2-167
eap 2-167
ieee8021x provisioning 2-167

Provisioning discovery context 2-168
end 2-168
dns name 2-168
dns provisioning 2-168
inherit 2-168
dns domain name 2-168
dns server 2-169
discovery provisioning 2-169
ip address 2-169
ip provisioning 2-169

Wireless interface context 2-170
dot11 2-170
distance 2-170
transmit power 2-171
multicast rate 2-171
dot11 automatic frequency 2-171
dot11 automatic frequency period 2-171
dot11 automatic frequency time 2-171
dot11 automatic transmit-power 2-172
dot11 automatic transmit-power period 2-172
antenna bidirectionnal 2-172
antenna gain 2-172

autochannel skip 2-172
station distance 2-172
beacon interval 2-173
rts threshold 2-173
dot11 mode 2-173
radio active 2-173
spectralink view 2-174
New client statistics 2-174
dot11n guard interval 2-174
dot11n mimo 2-174
dot11n channel width 2-174
dot11n channel extension 2-174
dot11n mac protection 2-175
end 2-175
inherit 2-175

RADIUS profile context 2-176
end 2-176
inherit 2-176
radius nas id 2-176

Local mesh profile context 2-177
security 2-177
security mode 2-177
security psk 2-177
security wep 2-177
dynamic mode 2-177
mesh id 2-178
allowed downtime 2-178
minimum snr 2-178
snr cost per hop 2-178
initial discovery time 2-178
active 2-179
end 2-179
inherit 2-179
name 2-179
radio active 2-179

Local mesh provisioning context 2-180
accept connection 2-180
end 2-180

inherit 2-180
multiple radio 2-180
Switch port context 2-181
end 2-181
active 2-181
app-profile 2-181
app-profile 2-181
authentication profile vsc 2-181
authentication server radius 2-182
dot1x authentication 2-182
dynamic vlan 2-182
egress rate 2-182
force flow control 2-182
ingress rate 2-183
ingress traffic type 2-183
loop protection 2-183
mac authentication 2-183
mac filter list 2-183
poe-class-support 2-183
port name 2-184
port type 2-184
power over ethernet 2-184
priority 2-184
priority lookup 2-184
quarantine vlan 2-184
secondary vlan 2-185
vlan 2-185
MAC addresses list context 2-186
end 2-186
entry 2-186
list name 2-186
Network profile context 2-187
end 2-187
name 2-187
vlan 2-187
vlan 2-187
New default 2-187

LLDP agent context 2-188
admin-status 2-188
basic-tlv-enable 2-188
basic-tlv-enable port_desc 2-188
basic-tlv-enable system_cap 2-188
basic-tlv-enable system_descr 2-188
basic-tlv-enable system_name 2-189
dot3-tlv-enable 2-189
end 2-189
ip-addr-enable 2-189
med-application-type 2-189
medtlv-enable capabilities 2-189
medtlv-enable location-id 2-190
medtlv-enable network-policy 2-190
medtlv-enable poe 2-190

Alphabetical list of commands

accept connection 2-180
access control 2-99
access controlled 2-144
access controlled 2-79
access controlled 2-85
access controller shared secret 2-39
access controller 2-40
access lan stations 2-110
access level 2-142
access list 2-79
access-controlled profile 2-144
access-controlled profile 2-85
access-controlled virtual ap 2-144
access-controlled virtual ap 2-85
access-list 2-69
accounting interim update 2-75
accounting interim update 2-79
active 2-109
active 2-127
active 2-129
active 2-132
active 2-135
active 2-145
active 2-179
active 2-181
active 2-86
active 2-98
active-directory check attribute 2-54
active-directory check user access 2-55
active-directory device name 2-55
active-directory domain netbios name 2-55
active-directory domain 2-55
active-directory group name 2-145
active-directory group order 2-55
active-directory group 2-55
active-directory join 2-56
add ip-qos profile 2-111
admin local authentication 2-14
admin radius authentication server 2-15
admin radius authentication 2-15
admin-status 2-188
ads presentation interval 2-62
ads presentation with frameset 2-65
ads presentation 2-62
allowed downtime 2-178
anonymous identity 2-167
antenna bidirectionnal 2-172
antenna gain 2-172
ap group 2-147
ap name 2-147
app-profile 2-181
app-profile 2-181
arp polling interval 2-80
arp polling max count 2-80
arp 2-6
arping 2-3
arping 2-6
authentication http 2-66
authentication https 2-66
authentication profile vsc 2-181
authentication server access controller 2-102
authentication server accounting radius profile 2-102
authentication server accounting 2-102
authentication server radius 2-102
authentication server radius 2-182
authentication server request radius cui 2-103
authentication 2-129
authorize_net installation id 2-64
authorize_net payment url 2-64
authorize_net transaction key 2-64
autochannel skip 2-172
band steering 2-109
New bandwidth control high 2-49
bandwidth control internet-port high 2-47
bandwidth control internet-port low 2-47
bandwidth control internet-port max-rate 2-47
bandwidth control internet-port normal 2-48
bandwidth control internet-port very-high 2-48
bandwidth control internet-port 2-47
New bandwidth control low 2-49
New bandwidth control max-rate 2-49
New bandwidth control normal 2-50
New bandwidth control very-high 2-50
New bandwidth control 2-49
bandwidth default rates maximum 2-114
bandwidth default rates 2-113
bandwidth level 2-80
bandwidth 2-113
basic-tlv-enable port_desc 2-188
basic-tlv-enable system_cap 2-188
basic-tlv-enable system_descr 2-188
basic-tlv-enable system_name 2-189
basic-tlv-enable 2-188
beacon dtim count 2-109
beacon interval 2-173
beacon transmit power 2-110
bridge protocol ieee vlan 2-156
bridge protocol ieee 2-156
broadcast filter 2-110
cap-switch to 2-13
certificate binding 2-10
certificate ipsec ca 2-40
certificate ipsec local 2-40
certificate ipsec revocation 2-41
certificate revocation 2-11
certificate ssl 2-41
certificate 2-10
chargeable user identity 2-86
cipher 2-129
client data tunnel security 2-57
New client statistics 2-174
clock auto adjust dst 2-22
clock custom dst begins format 2-23
clock custom dst begins 2-23
clock custom dst ends format 2-24
clock custom dst ends 2-24
clock timezone 2-22
clock use custom dst rules 2-22
clock 2-22
community 2-143
config file 2-70
config 2-147
config 2-149
config 2-150
config 2-9
config-update automatic 2-25

config-update operation ... 2-25
config-update start ... 2-25
config-update time ... 2-25
config-update url ... 2-25
config-update weekday ... 2-25
config-version ... 2-53
console authentication ... 2-18
contact ... 2-148
control method ... 2-86
controlled network ... 2-9
country code ... 2-167
credentials ... 2-98
daily restriction ... 2-139
data rate ... 2-110
New default ... 2-187
delete ip-qos profile all ... 2-111
delete ip-qos profile ... 2-111
dhcp mode ... 2-18
dhcp public ip default lease period ... 2-10
dhcp public ip subnet ... 2-10
New dhcp relay access access network ... 2-21
dhcp relay access centralized clients ... 2-21
dhcp relay access lan ... 2-21
dhcp relay active ... 2-115
dhcp relay circuit id ... 2-115
dhcp relay circuit id ... 2-20
New dhcp relay extend internet network ... 2-22
dhcp relay extend internet port ... 2-21
dhcp relay remote id ... 2-115
dhcp relay remote id ... 2-21
dhcp relay subnet ... 2-115
dhcp relay ... 2-115
dhcp relay ... 2-20
dhcp server access centralized clients ... 2-20
dhcp server access lan ... 2-20
dhcp server controller discovery ... 2-19
dhcp server controller ... 2-19
dhcp server default domain name ... 2-19
dhcp server default lease period ... 2-19
dhcp server default permanent lease period ... 2-19
dhcp server dns ... 2-116
dhcp server gateway ... 2-116
dhcp server logout html user ... 2-20
dhcp server range ... 2-116
dhcp server subnet ... 2-116
dhcp server ... 2-116
dhcp server ... 2-19
disassociate controlled-ap wireless client ... 2-8
discovery protocol device-id ... 2-44
discovery protocol ... 2-44
discovery provisioning ... 2-169
distance ... 2-170
dns domain name ... 2-168
dns domain ... 2-129
dns name ... 2-168
dns provisioning ... 2-168
dns server ... 2-129
dns server ... 2-169
dot11 automatic frequency period ... 2-171
dot11 automatic frequency time ... 2-171
dot11 automatic frequency ... 2-171
dot11 automatic transmit-power period ... 2-172
dot11 automatic transmit-power ... 2-172
dot11 mode ... 2-173
dot11 ... 2-170
dot11n channel extension ... 2-174
dot11n channel width ... 2-174
dot11n guard interval ... 2-174
dot11n mac protection ... 2-175
dot11n mimo ... 2-174
dot1x authentication ... 2-102
dot1x authentication ... 2-182
New dot1x radius accounting start delay ... 2-51
dot1x reauth period ... 2-155
dot1x reauth period ... 2-52
dot1x reauth terminate ... 2-155
dot1x reauth terminate ... 2-52
dot1x reauth ... 2-155
dot1x reauth ... 2-52
dot1x session page ... 2-103
dot1x supplicant timeout ... 2-156
dot1x supplicant timeout ... 2-52
dot3-tlv-enable ... 2-189
dual radio binding ... 2-162
duplex ... 2-89
duplex ... 2-91
New duplex-mode ... 2-118
dynamic key interval ... 2-155
dynamic key interval ... 2-53
dynamic key ... 2-155
dynamic key ... 2-52
dynamic mode ... 2-177
dynamic vlan ... 2-182
eap ... 2-167
egress rate ... 2-182
egress unauthenticated ... 2-100
egress vlan ... 2-145
egress vlan ... 2-162
egress vlan ... 2-162
egress vlan ... 2-80
egress vlan ... 2-86
enable console password reset ... 2-18
enable vsc services ... 2-157
enable ... 2-3
encryption key 1 ... 2-101
encryption key format ... 2-101
end force ... 2-128
end time ... 2-139
end time ... 2-86
end ... 2-11
end ... 2-117
New end ... 2-118
end ... 2-120
end ... 2-122
end ... 2-125
end ... 2-127
end ... 2-129
end ... 2-133
end ... 2-135
end ... 2-137
end ... 2-138
end ... 2-139
end ... 2-142
end ... 2-143
end ... 2-144
end ... 2-147
end ... 2-149
end ... 2-150
end ... 2-151
end ... 2-162
end ... 2-164
end ... 2-165

end ... 2-168
end ... 2-175
end ... 2-176
end ... 2-179
end ... 2-180
end ... 2-181
end ... 2-186
end ... 2-187
end ... 2-189
end ... 2-6
end ... 2-62
end ... 2-77
end ... 2-79
end ... 2-85
end ... 2-89
end ... 2-91
end ... 2-95
end ... 2-97
end ... 2-98
end-port ... 2-125
entry ... 2-186
execute action ... 2-147
execute action ... 2-149
execute action ... 2-150
execute system action ... 2-147
factory settings ... 2-11
fail page ... 2-71
fast authentication ... 2-110
firewall mode ... 2-51
firmware-update automatic ... 2-37
firmware-update start ... 2-37
firmware-update time ... 2-37
firmware-update uri ... 2-37
firmware-update weekday ... 2-38
New flow-control auto-negotiation ... 2-118
New flow-control ... 2-118
force centralize data ... 2-99
force flow control ... 2-182
gateway ... 2-127
goodbye url ... 2-71
gre name ... 2-128
group name ... 2-149
guest-mode ... 2-100
html authentication accounting radius profile ... 2-108
html authentication accounting ... 2-108
html authentication active-directory ... 2-108
html authentication local ... 2-108
html authentication radius profile ... 2-108
html authentication radius ... 2-108
html authentication request radius cui ... 2-109
html authentication timeout ... 2-109
html authentication ... 2-107
html redirection ... 2-113
http proxy upstream ... 2-71
https ssl certificate ... 2-71
identify stations by ip only ... 2-114
idle timeout ... 2-75
idle timeout ... 2-81
idle timeout ... 2-86
ieee8021x provisioning ... 2-167
igmp proxy downstream interface ... 2-57
igmp proxy upstream interface ... 2-57
igmp proxy ... 2-57
incoming nat ... 2-130
incoming traffic network ... 2-130
ingress interface ... 2-100
ingress rate ... 2-183
ingress traffic type ... 2-183
inherit 8021x ... 2-156
inherit country code ... 2-152
New inherit ipv6 ra conversion ... 2-153
inherit l3subnets ... 2-158
inherit lldp-app-profile ... 2-158
inherit lldp-general ... 2-159
inherit local mesh qos ... 2-157
inherit sensor ... 2-154
inherit service availability ... 2-157
inherit switch port _ ... 2-158
inherit switch ports ... 2-158
inherit untagged stp ... 2-156
inherit vlan port2 ... 2-152
inherit vlan stp ... 2-157
inherit ... 2-164
inherit ... 2-165
inherit ... 2-168
inherit ... 2-175
inherit ... 2-176
inherit ... 2-179
inherit ... 2-180
initial discovery time ... 2-178
initial login time allocation ... 2-139
intercept traffic ... 2-81
interface ethernet ... 2-12
interface gre ... 2-12
interface ip ... 2-12
interface pptp client-default ... 2-12
interface provisioning ... 2-165
interface vlan ... 2-89
interface vlan ... 2-91
interface wireless ... 2-151
New interface ... 2-10
interface ... 2-130
interface ... 2-165
interval ... 2-98
ip address alternate ... 2-96
ip address dhcp client-id ... 2-94
ip address management ... 2-97
ip address mode ... 2-120
ip address mode ... 2-93
ip address ... 2-120
ip address ... 2-128
ip address ... 2-169
ip address ... 2-94
ip address ... 2-97
ip assignation ... 2-165
ip default-gateway ... 2-121
ip http port ... 2-15
ip https port ... 2-15
ip name-server cache ... 2-38
ip name-server dynamic ... 2-38
ip name-server interception ... 2-39
ip name-server logout-info ... 2-39
ip name-server switch-on-servfail ... 2-39
ip name-server switch-over ... 2-39
ip name-server ... 2-38
ip nat outside source static ... 2-96
ip nat ... 2-121
ip nat ... 2-135
ip nat ... 2-94
ip provisioning ... 2-169
ip route gateway ... 2-50
ip-addr-enable ... 2-189

ipass id ... 2-68
ipass login url ... 2-72
ipass name ... 2-68
iperf ... 2-5
ip-qos profile ... 2-40
ipsec policy ... 2-14
ipsec vlan interface ... 2-90
ipsec vlan interface ... 2-92
New ipv6 ra conversion ... 2-153
key chain name ... 2-137
key chain ... 2-53
key ... 2-137
key-string ... 2-138
l3subnet ... 2-158
layer3 mobility hns fallback method ... 2-111
layer3 mobility hns method ... 2-111
layer3 mobility ... 2-111
level ... 2-133
level ... 2-133
level ... 2-163
level ... 2-164
list name ... 2-186
lldp app-profile ... 2-159
lldp app-profile ... 2-159
lldp app-profile ... 2-159
lldp app-profile ... 2-159
lldp config ... 2-42
lldp dynamic-name refresh-time ... 2-42
lldp dynamic-name user-string ... 2-42
lldp dynamic-name ... 2-159
lldp dynamic-name ... 2-42
lldp fast-start-count ... 2-160
lldp fast-start-count ... 2-42
lldp holdtime-multipher ... 2-160
lldp holdtime-multipher ... 2-43
lldp local-mesh ... 2-160
lldp med-location civic-address-element ... 2-160
lldp med-location civic-address-element ... 2-43
lldp med-location elin-addr ... 2-160
lldp med-location elin-addr ... 2-43
lldp refresh-interval ... 2-160
lldp refresh-interval ... 2-43
lldp run ... 2-161
lldp run ... 2-43
local id ... 2-130
local mesh group ... 2-151
local mesh ip qos profile ... 2-157
local mesh provisioning group ... 2-151
local mesh qos mechanism ... 2-157
local nas id ... 2-113
local welcome-page ... 2-56
location aware ... 2-162
location ... 2-148
location-aware called-station-id content ... 2-115
location-aware group ... 2-114
logging destination ... 2-26
logging facility ... 2-132
logging host ... 2-132
logging prefix ... 2-132
logging source ... 2-133
login error url ... 2-72
login page ... 2-72
login url ... 2-72
logo ... 2-72
loop protection ... 2-183
mac authentication accounting radius profile ... 2-106
mac authentication accounting ... 2-106
mac authentication local ... 2-107
mac authentication radius profile ... 2-106
mac authentication remote ... 2-107
mac authentication request radius cui ... 2-107
mac authentication ... 2-107
mac authentication ... 2-183
mac filter list ... 2-183
mac list ... 2-14
mac lockout entry ... 2-59
mac-address ... 2-71
mac-filters local ... 2-105
mac-filters mode ... 2-106
mac-filters ... 2-106
matches ... 2-133
matches ... 2-164
max input rate ... 2-81
max output rate ... 2-81
max user sessions ... 2-87
max-association ... 2-100
maximum input octets ... 2-75
maximum input packets ... 2-75
maximum output octets ... 2-76
maximum output packets ... 2-76
maximum total octets ... 2-76
maximum total packets ... 2-76
med-application-type ... 2-189
medtlv-enable capabilities ... 2-189
medtlv-enable location-id ... 2-190
medtlv-enable network-policy ... 2-190
medtlv-enable poe ... 2-190
mesh id ... 2-178
message ... 2-134
message ... 2-134
message ... 2-163
message ... 2-163
messages ... 2-73
minimum snr ... 2-178
mode ... 2-130
multicast rate ... 2-171
multiple radio ... 2-180
name ... 2-132
name ... 2-179
name ... 2-187
nat limit port range size ... 2-94
nat limit port range ... 2-94
nat one-to-one ... 2-76
nat one-to-one ... 2-82
network-profile ... 2-11
noc access interface gre ... 2-68
noc access interface vlan ... 2-68
noc access internet ... 2-66
noc access vpn ... 2-66
noc allow ... 2-66
noc authentication ... 2-67
noc ssl ca-certificate ... 2-73
noc ssl certificate ... 2-73
notify user location changes ... 2-74
nslookup ... 2-3
ntp protocol ... 2-23
ntp server failure trap ... 2-24
ntp server ... 2-23
ntp server ... 2-24
online time limit ... 2-140
online time limit ... 2-140
outgoing traffic network ... 2-130

password ... 2-142
password ... 2-87
paypal api-url ... 2-65
paypal operation-mode ... 2-65
paypal password ... 2-65
paypal signature ... 2-65
paypal user-id ... 2-65
peer id ... 2-130
peer ip address ... 2-128
peer ip address ... 2-131
perfect forward secrecy ... 2-131
permanent leases ... 2-127
persistent user information period ... 2-57
persistent user information ... 2-57
ping ... 2-3
ping ... 2-6
poe-class-support ... 2-183
port name ... 2-184
port type ... 2-184
port ... 2-143
power over ethernet ... 2-184
pppoe auto-reconnect ... 2-95
pppoe client user ... 2-93
pppoe mru ... 2-95
pppoe mtu ... 2-95
pppoe unnumbered ... 2-95
pptp client auto route discovery ... 2-136
pptp client credentials ... 2-135
pptp client domain name ... 2-135
pptp client lcp echo ... 2-136
pptp client server address ... 2-135
preshared key ... 2-131
priority lookup ... 2-184
priority ... 2-125
priority ... 2-184
process ... 2-134
process ... 2-134
process ... 2-163
process ... 2-163
product type ... 2-148
product type ... 2-148
profile name ... 2-125
protocol ... 2-125
provisioning connectivity ... 2-151
provisioning discovery ... 2-151
provisioning local mesh group ... 2-166
provisioning local mesh key ... 2-166
provisioning local mesh port ... 2-166
provisioning local mesh security ... 2-166
provisioning local mesh security ... 2-167
provisioning local mesh type ... 2-167
ps ... 2-3
public forwarding ... 2-110
public ip reservation ... 2-140
public ip subnet ... 2-140
public ip subnet ... 2-77
public ip subnet ... 2-83
qos ... 2-112
quarantine vlan ... 2-184
quit ... 2-3
quit ... 2-6
radio active ... 2-173
radio active ... 2-179
radius accounting realms ... 2-114
radius authentication realms ... 2-114
radius nas id ... 2-176
radius profile ... 2-151
radius server profile ... 2-98
radius-framed-protocol-attribute ... 2-116
radius-server accounting port ... 2-122
radius-server accounting session ... 2-53
radius-server alternate hosts ... 2-122
radius-server authentication method ... 2-122
radius-server authentication port ... 2-122
radius-server client ... 2-53
radius-server client ... 2-56
radius-server deadtime ... 2-123
radius-server force-nas-port-to-vlanid ... 2-124
radius-server host ... 2-123
radius-server key 2 ... 2-123
radius-server local eap-peap ... 2-53
radius-server local eap-tls ... 2-54
radius-server local eap-ttls ... 2-54
radius-server local pap ... 2-54
radius-server message-authenticator ... 2-123
radius-server name ... 2-123
radius-server nasid ... 2-124
radius-server profile ... 2-40
radius-server realm name ... 2-124
radius-server realm ... 2-124
radius-server ssid detection nas-id ... 2-54
radius-server timeout ... 2-124
radius-server timeout ... 2-124
range ... 2-127
rcapture ... 2-6
reboot device ... 2-11
reboot device ... 2-5
receiver ... 2-143
regular profile ... 2-145
regular profile ... 2-87
regular virtual ap ... 2-145
regular virtual ap ... 2-87
remember delay ... 2-63
remember html users ... 2-64
remote configuration ... 2-41
remote ip address ... 2-128
renew user profile subscription ... 2-51
rf-id aeroscout ... 2-58
rts threshold ... 2-173
secondary vlan ... 2-185
secure login ... 2-67
security mode ... 2-177
security psk ... 2-177
security wep ... 2-177
security ... 2-117
security ... 2-142
security ... 2-177
sensor discovery mode ... 2-154
sensor network detector ... 2-154
sensor server id ... 2-154
sensor server name ... 2-153
service controller ap authentication credentials ... 2-44
service controller ap authentication enable ... 2-44
service controller ap authentication file ... 2-45
service controller ap authentication radius-server ... 2-45
service controller ap authentication refresh-rate ... 2-45
service controller ap authentication source file ... 2-45
service controller ap authentication source local ... 2-45
service controller ap authentication source radius ... 2-45
service controller discovery interface internet-port ... 2-46
service controller discovery interface lan-port ... 2-46
New service controller discovery interface ... 2-47

service controller discovery ... 2-46
service controller primary ip addr ... 2-46
service controller primary ... 2-46
service controller priority ... 2-46
service controller provisioning ... 2-47
session page ... 2-73
session profile default ... 2-41
session profile ... 2-41
session profile ... 2-82
session timeout ... 2-77
session timeout ... 2-87
sflow destination 80211 ... 2-58
sflow interface ... 2-59
sflow polling ... 2-59
sflow sampling ... 2-59
sflow ... 2-58
show active-directory group ... 2-56
show active-directory ... 2-56
show all config ... 2-9
show arp ... 2-6
show bridge forwarding ... 2-7
show bridge ... 2-7
show certificate binding ... 2-11
show certificate binding ... 2-5
show certificate ... 2-11
show certificate ... 2-5
show client log ... 2-8
show config factory ... 2-12
show config factory ... 2-147
show config factory ... 2-149
show config factory ... 2-150
show controlled network config ... 2-9
show controlled-aps wireless clients ... 2-8
show discrete pin ... 2-9
show dns cache ... 2-7
show interfaces ... 2-7
show ip dhcp database ... 2-8
show ip route ... 2-7
show ip ... 2-7
New show ipv6 ra conversion ... 2-153
New show lacp ... 2-13
show license ... 2-4
show lldp config ... 2-43
show lldp info local-device ... 2-43
show lldp info remote-device ... 2-44
show lldp stats ... 2-44
show logging filtered ... 2-4
show mac list ... 2-14
show mac lockout ... 2-59
New show mac-address count ... 2-13
New show mac-address ... 2-13
show network-profiles ... 2-12
show paypal ... 2-65
show radius statistics ... 2-8
show radius users ... 2-8
show radius-server ... 2-54
show satellites ... 2-8
show session profile ... 2-41
show sflow agent ... 2-58
show sflow controller stats ... 2-58
show sflow destination ... 2-58
show sflow device stats ... 2-58
show sflow sampling-polling ... 2-59
show subscription plan ... 2-14
show system info ... 2-7
show tech ... 2-12
show tech ... 2-152
New show trunks ... 2-13
show user profiles details ... 2-51
show user profiles ... 2-51
show users ... 2-9
New show vlans ... 2-13
show vsc overview ... 2-7
show web content ... 2-8
smtp redirection setup ... 2-77
smtp redirection setup ... 2-82
smtp redirection ... 2-78
snmp-server access interface gre ... 2-30
snmp-server access interface vlan ... 2-30
snmp-server access lan ... 2-33
snmp-server access port-1 ... 2-30
snmp-server access port-2 ... 2-31
snmp-server access vpn ... 2-31
snmp-server allow ... 2-27
snmp-server chassis-id ... 2-27
snmp-server contact ... 2-27
snmp-server heartbeat period ... 2-27
snmp-server location ... 2-27
snmp-server notification receiver ... 2-33
snmp-server port ... 2-28
snmp-server readonly ... 2-28
snmp-server readwrite ... 2-28
snmp-server trap certificate-expired ... 2-15
snmp-server trap certificate-expires-soon ... 2-16
snmp-server trap community ... 2-28
snmp-server trap config-change ... 2-26
snmp-server trap config-update ... 2-26
snmp-server trap destination ... 2-29
snmp-server trap device-authorization-failure ... 2-31
snmp-server trap device-configuration-failure ... 2-31
snmp-server trap device-firmware-failure ... 2-31
snmp-server trap device-security-failure ... 2-32
snmp-server trap device-state-change ... 2-32
snmp-server trap firmware-update ... 2-38
snmp-server trap heartbeat ... 2-29
snmp-server trap link-state ... 2-29
snmp-server trap network-trace ... 2-36
snmp-server trap new-satellite-detected ... 2-32
snmp-server trap satellite-unreachable ... 2-32
snmp-server trap service-controller-state ... 2-32
snmp-server trap snmp-authentication ... 2-29
snmp-server trap syslog-matches regex ... 2-36
snmp-server trap syslog-matches ... 2-36
snmp-server trap syslog-severity level ... 2-36
snmp-server trap syslog-severity ... 2-26
snmp-server trap vpn-connection ... 2-36
snmp-server trap web-fail ... 2-16
snmp-server trap web-login ... 2-16
snmp-server trap web-logout ... 2-16
snmp-server trap ... 2-28
snmp-server user ... 2-33
snmp-server version 1 ... 2-29
snmp-server version 2c ... 2-30
snmp-server version 3 ... 2-30
snmp-server ... 2-26
snr cost per hop ... 2-178
soap-server access interface gre ... 2-35
soap-server access interface vlan ... 2-33
soap-server access lan ... 2-35
soap-server access port-1 ... 2-35
soap-server access port-2 ... 2-35
soap-server access vpn ... 2-36

soap-server allow ... 2-34
soap-server http authentication password ... 2-34
soap-server http authentication username ... 2-34
soap-server http authentication ... 2-34
soap-server port ... 2-34
soap-server ssl with client certificate ... 2-35
soap-server ssl ... 2-34
soap-server ... 2-33
spectralink view ... 2-174
New speed ... 2-118
speed ... 2-89
speed ... 2-91
ssid name ... 2-101
sslv2 authentication ... 2-67
start time ... 2-140
start-port ... 2-125
static ip ... 2-166
station distance ... 2-172
station free access ... 2-62
station http proxy html authentication only support 2-62
station http proxy support ... 2-63
station idle detection ... 2-63
subscription plan name ... 2-140
subscription plan ... 2-14
subscription plan ... 2-88
switch port ... 2-152
syslog ... 2-152
system accounting ... 2-63
New tagged ... 2-120
New tagged ... 2-93
New tagged ... 2-97
New team communication interface ... 2-60
New team communication interface ... 2-60
New team communication ip address ... 2-59
New team communication vlan ... 2-60
New team communication vlan ... 2-61
team management address ... 2-60
team management interface vlan ... 2-61
team management interface ... 2-61
team manager ... 2-60
New team name ... 2-60
teaming ... 2-60
termination action ... 2-83
top ... 2-4
traceroute ... 2-4
transmit key ... 2-101
transmit power ... 2-171
transport page ... 2-73
New trunk group ... 2-118
New trunk type ... 2-119
New untagged ... 2-120
New untagged ... 2-93
New untagged ... 2-97
upstream diffserv tagging ... 2-113
use access-list unauth ... 2-70
use access-list ... 2-70
user defined attribute ... 2-83
user name ... 2-142
user profile ... 2-51
user tracking destination ... 2-56
user tracking filter ... 2-56
user tracking port ... 2-57
user tracking ... 2-56
user ... 2-143
user-agent block ... 2-67
user-agent filtering ... 2-67
username ... 2-16
username ... 2-88
version ... 2-143
virtual ap binding ... 2-149
virtual ap name ... 2-99
virtual ap ... 2-13
vlan port2 id ... 2-152
vlan port2 ... 2-152
vlan ... 2-10
vlan ... 2-166
vlan ... 2-166
vlan ... 2-185
vlan ... 2-187
vlan ... 2-187
web access interface gre ... 2-18
web access interface vlan ... 2-17
web access internet-port ... 2-17
web access lan ... 2-18
web access lan-port ... 2-17
web access vpn ... 2-18
web admin kickout ... 2-17
web allow ... 2-17
welcome url ... 2-74
wireless filters mac ... 2-103
wireless filters rule input ... 2-104
wireless filters rule output ... 2-104
wireless filters type ... 2-104
wireless filters ... 2-103
wispr abort login url ... 2-68
wispr login url ... 2-69
wispr logoff url ... 2-69
wmm advertising ... 2-113
world-mode dot11 country code ... 2-153
worldpay installation id ... 2-64
worldpay payment response password ... 2-64
worldpay payment url ... 2-64
New wpa terminate controller ... 2-103
wpa-psk ... 2-102

1

Introduction

Contents

About this guide 1-2
- Products covered 1-2
- Important terms 1-2
- Typographical conventions 1-2

New in this release 1-4

HP support 1-4

Online documentation 1-5

Configuring CLI support 1-5
- Secure shell access 1-6
- Authentication 1-6
- Serial port access 1-7

Entering strings 1-8

Context hierarchy 1-9

Sample CLI sessions 1-10

File transfer 1-12

About this guide

This guide explains how to work with the Command Line Interface (CLI) on HP MSM7xx Controllers.

Products covered

This guide covers the following products:

Model	Part
MSM710 Access Controller	J9328A
MSM710 Mobility Controller	J9325A
E-MSM720 Access Controller	J9693A
E-MSM720 Premium Mobility Controller	J9694A
MSM760 Access Controller	J9421A
MSM760 Premium Mobility Controller	J9420A
MSM765zl Premium Mobility Controller	J9370A

Important terms

The following terms are used in this guide.

Term	Description
AP	Refers to any HP MSM3xx or MSM4xx Access Point.
controller, service controller	Refers to any HP MSM7xx Controller, including both Access Controller and Mobility Controller variants.
VSC, Virtual ap, VAP	These terms are used interchangeably to refer to VSC (Virtual Service Community).

Typographical conventions

Command syntax

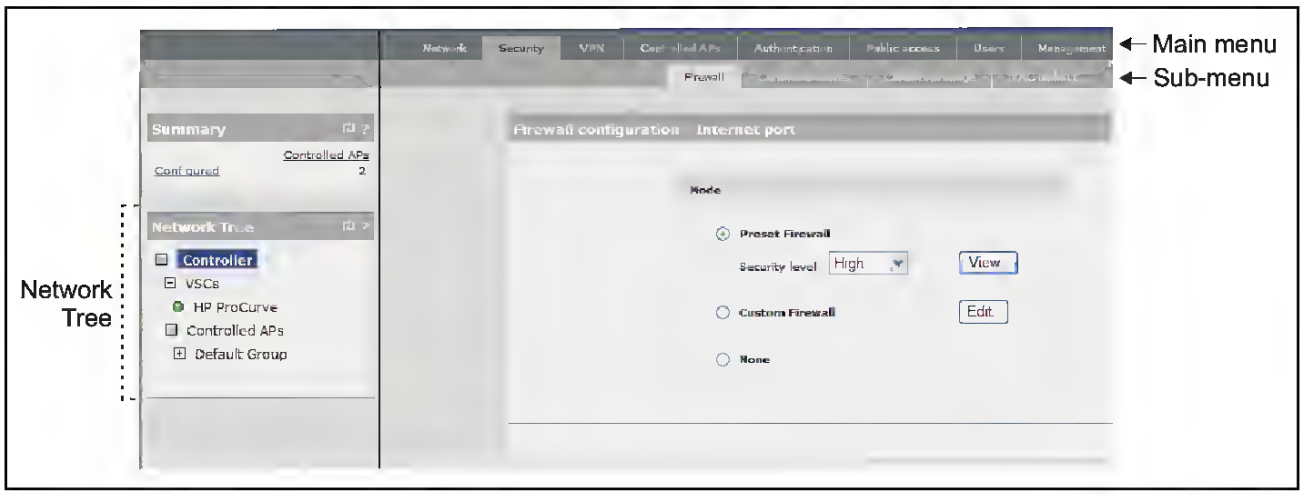
Command syntax is formatted in a monospaced font as follows:

Example	Description
`web admin kickout`	Items in plain text must be entered as shown.
`ip http port <number>`	Items in italics and enclosed in < > are parameters for which you must supply a value. In this example, you must supply a value for *<number>*.

Example	Description
`end [force]`	Items enclosed in square brackets are optional. You can either include them or not. Do not include the brackets. In this example you can either include "force" or omit it.
`firewall mode (high|low|none)`	Items enclosed in parenthesis and separated by a vertical line indicate a choice. Specify only one of the items. In this example, you must specify 'high', 'low', or 'none'.

Management tool

This guide uses specific syntax when directing you to interact with the management tool user interface on the controller. Key user-interface elements are identified as follows:



Example directions in this guide	What to do in the user interface
Select **Controller >> Security > Firewall**.	**On a non-teamed MSM7xx controller** In the Network Tree select the **Controller** element, then on the main menu select **Security,** and then select **Firewall** on the sub-menu. All elements to the left of the double angle brackets **>>** are found in the Network Tree. **On an MSM7xx controller team** In the Network Tree on the team manager, select the **Team [*team-name*]** element, then on the main menu select **Security,** and then select **Firewall** on the sub-menu. All elements to the left of the double angle brackets >> are found in the Network Tree.

Example directions in this guide	What to do in the user interface
Select **Controller > VSCs > [*VSC-name*] >> Configuration**.	**On a non-teamed MSM7xx controller** Expand the **Controller** branch (click its + symbol), expand the **VSCs** branch, select a **[*VSC-name*]**, then select **Configuration** on the main menu. **On an MSM7xx controller team** In the Network Tree on the team manager, expand the **Team: [*team-name*]** branch (click its + symbol), expand the **VSCs** branch, select a **[*VSC-name*]**, then select **Configuration** on the main menu.
For **Password** specify **secret22**.	In the **Password** field enter the text **secret22** exactly as shown.

New in this release

New CLI commands in this release are identified by the text New in the left margin. This is done in the table of contents, alphabetical list of commands, and *Chapter 2: CLI commands*.

HP support

For support information, visit www.hp.com/networking/support and for **Product Brand**, select **ProCurve**. Additionally, your HP-authorized networking products reseller can provide you with assistance.

Before contacting support

To make the support process most efficient, before calling your networking dealer or HP Support, you first should collect the following information:

Collect this information	Where to find it
Product identification.	On the rear of the product.
Software version.	The service controller management tool **Login** page.
Network topology map, including the addresses assigned to all relevant devices.	Your network administrator.

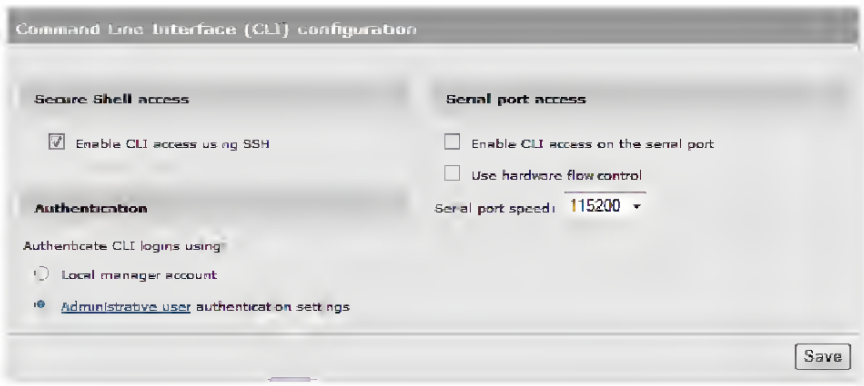
Online documentation

You can download documentation from the HP Support Website at: www.hp.com/support/manuals.

Search by product name or part number.

Configuring CLI support

CLI support is configured using the management tool on the controller. Select **Controller >> Management > CLI** to open the **Command Line Interface (CLI) configuration** page.



Note

A maximum of three concurrent CLI sessions are supported.

Secure shell access

Enable this option to allow access to the CLI via an SSH session. The CLI supports SSH on the standard TCP port (22).

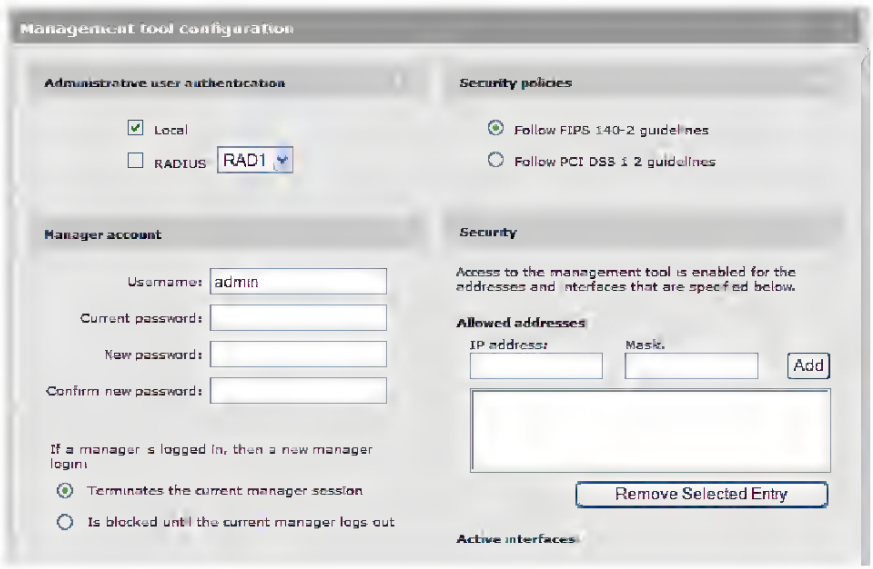
SSH connections to the CLI can be made on any active interface. Support for each interface must be explicitly enabled under **Security** on the **Controller >> Management > Management tool** page.

The following SSH clients have been tested with the CLI. Others may work as well:

- OpenSSH
- Tectia
- SecureCRT
- Putty

Authentication

The CLI validates login credentials (username and password) using the settings defined under **Administrative user authentication** on the **Controller >> Management > Management tool** page (shown here for reference).



Local manager account

The login username and password are the same as those defined for the **local manager account**. If this account is disabled, the last known username and password for this account are used.

Administrative user authentication settings

The login username and password use the same settings (**Local** and/or **RADIUS**) as defined for the manager account.

Serial port access

Access to the CLI via the console port is available on the MSM710 and MSM760.

Enable the CLI on serial port

When enabled, access to the command line interface is permitted via the serial port.

Use hardware flow control

Enables hardware flow control.

Serial port line speed

Speed of the serial port connection.

Starting a CLI session on the serial port

The following step sequence illustrates how to start a CLI session via a serial connection to the controller.

1. Power off the controller.
2. Connect a serial cable to the controller console port as follows:
   - For the MSM710, see *Console ports* in the *MSM7xx Configuration Guide.*
   - For the MSM760, see the *MSM760 Controllers Installation Guide.*
3. Configure a communications terminal program (such as Microsoft Hyperterminal for Windows, or Minicom for Linux) as follows:
   - **Terminal**: VT-100 (ANSI)
   - **Speed**: Set speed according to **Serial port speed** option (**Management > CLI**):
   - **Data bits**: 8
   - **Stop bits**: 1
   - **Parity**: none
   - **Flow control**: none
4. Open an appropriately-configured terminal session.
5. Power on the controller. System boot messages appear.
6. Wait for the login prompt to appear.

   ```
   login:
   ```

7. Type the login username and press Enter.
8. The password prompt appears.

   ```
   password:
   ```

9. Type the login password and press Enter.
10. The CLI prompt appears. You can now enter CLI commands.

```
CLI>
```

Entering strings

When entering a value that contains spaces, you must enclose it in quotation marks. For example, if the command syntax is:

```
ssid <name>
```

You must specify one of the following:

```
ssid ANameWithNoSpaces
ssid "A name with spaces"
```

Context hierarchy

CLI commands are grouped into functional contexts. The following table shows the context hierarchy and the commands used to switch from the parent context:

Context hierarchy	To switch to this context from parent context
View	*(This is the root context. No command is needed.)*
Enable	`enable`
Config	`config`
VLAN interface	`vlan <name>`
WAN IP interface	`interface ip wan`
LAN IP interface	`interface ip lan`
Upstream/WAN port interface	`interface ethernet port-2`
VLAN interface	`interface vlan <id>[-<id2>]`
Downstream/LAN port interface	`interface ethernet port-1`
VLAN interface	`interface vlan <id>[-<id2>]`
Wireless interface	`interface wireless`
Local mesh profile	`local mesh profile`
VLAN interface	`interface vlan <id>[-<id2>]`
PPTP client interface	`interface pptp client-default`
GRE interface	`interface gre <name>`
Virtual AP	`virtual ap <name>`
Subscription plan	`subscription plan <name>`
MAC addresses list	`mac list <name>`
Network profile	`network-profile <name>`
IPsec	`ipsec policy <name>`
DHCP server	`dhcp server lan`
Syslog	`logging destination <name>`
SNMP user	`snmp-server user <name>`
SNMP notification receiver	`snmp-server notification receiver <host>`
RADIUS profile	`radius-server profile <name>`
IP QOS	`ip-qos profile <name>`
Access Controller	`access controller`
Default user session profile	`session profile default`
Session profile	`session profile <name>`
Public access RADIUS attributes	`remote configuration radius`
LLDP agent	`lldp config <port>`
User account	`user profile <name>`
Keychain	`key chain <name>`
Keys	`key <number>`
Active Directory Group	`active-directory group <name>`
Controlled APs	`controlled network {ap <name> [<mac>]`
Controlled APs network configuration	`config`

Context hierarchy	To switch to this context from parent context
Wireless interface	`interface wireless (single|dual|triple) <number>`
RADIUS profile	`radius profile <profile>`
Local mesh profile	`local mesh group <group>`
Local mesh provisioning	`local mesh provisioning group`
Provisioning connectivity	`provisioning connectivity`
Provisioning discovery	`provisioning discovery`
Syslog	`syslog`
Switch port	`switch port <name>`
Controlled APs group	`controlled network (group <name> [<mac>]`
Controlled APs VSC binding	`virtual ap binding <profile>`
Controlled APs network configuration	`config`
Wireless interface	`interface wireless (single|dual|triple) <number>`
RADIUS profile	`radius profile <profile>`
Local mesh profile	`local mesh group <group>`
Local mesh provisioning	`local mesh provisioning group`
Provisioning connectivity	`provisioning connectivity`
Provisioning discovery	`provisioning discovery`
Syslog	`syslog`
Switch port	`switch port <name>`
Controlled APs base group	`controlled network base`
Controlled APs network configuration	`config`
Wireless interface	`interface wireless (single|dual|triple) <number>`
RADIUS profile	`radius profile <profile>`
Local mesh profile	`local mesh group <group>`
Local mesh provisioning	`local mesh provisioning group`
Provisioning connectivity	`provisioning connectivity`
Provisioning discovery	`provisioning discovery`
Syslog	`syslog`
Switch port	`switch port <name>`

Sample CLI sessions

Example 1

This sample CLI session shows you how to set the WAN port to use a static IP address, disable NAT, and add an alternate IP address. (The CLI prompt is shown in bold.)

```
CLI> enable
CLI# config
CLI(config)# interface ip wan
CLI(config-if-ip)# ip address 192.168.66.1/24
CLI(config-if-ip)# ip address mode static
```

```
CLI(config-if-ip)# no ip nat
CLI(config-if-ip)# ip address alternate 192.168.23.56
CLI(config-if-ip)# end
CLI(config)# end
CLI# quit
```

Example 2

This sample CLI session shows you how to create a static trunk on the E-MSM720 that is bound to a network profile called **static trunk** on port 2. The trunk is created on trunk group 1 using a VLAN ID of 900 (tagged).

```
CLI> enable
CLI# config
CLI(config)# network-profile "static trunk"
CLI(network-profile)# vlan 900
CLI(network-profile)# vlan
CLI(network-profile)# default
CLI(network-profile)# end
CLI(config)# interface 1
CLI(if)# trunk type trunk
CLI(if)# trunk group 1
CLI(if)# end
CLI(config)# interface 2
CLI(if)# trunk group 1
CLI(if)# trunk type trunk
CLI(if)# end
CLI(config)#
```

Example 3

This sample CLI session shows you how to create a dynamic trunk on the E-MSM720 that is bound to a network profile called **lacp trunk** on ports 5 and 6. The trunk is created using a VLAN ID of 800 (tagged).

```
CLI> enable
CLI# config
CLI(config)# network-profile "lacp trunk"
CLI(network-profile)# vlan 800
CLI(network-profile)# vlan
CLI(network-profile)# default
CLI(network-profile)# end
CLI(config)# interface 1
CLI(if)# trunk type lacp
CLI(if)# end
CLI(config)# interface 2
CLI(if)# trunk type lacp
CLI(if)# end
```

File transfer

In some cases you may need to transfer files (certificates or configuration) to the controller. Commands that have this capability typically include <uri> or <url> in their parameter list.

Note

When you enter the commands discussed here, the files are transferred immediately.

File transfer can be performed in two ways.

A. The controller gets the file using a URL

Transfer a certificate file using ftp. For example:

```
certificate ipsec ca ftp://ftp.example.com/certificate/my-root-certificate.pem
```

B. Send a file to the controller

Using SFTP (available with OpenSSH or SSH), authenticate with the CLI credentials. Then send the file to the controller. For example:

```
sftp msm710.mycompany.com
>login: admin
>password: ****
>put my-root-certificate.pem
file transferred (1k)
>quit
```

In the CLI, use the local://< > parameter in the URL. Replace < > with the filename you used to transfer using SFTP. For example:

```
CLI(config)# certificate ipsec ca local://my-root-certificate.pem
```

2

CLI commands

Contents

View context 2-3

Enable context 2-5

Config context 2-10

Access Controller context 2-62

Default user session profile context 2-75

Session profile context 2-79

User account context 2-85

Internet port interface context 2-89

LAN port interface context 2-91

WAN IP interface context 2-93

LAN IP interface context 2-97

Public access RADIUS attributes context 2-98

Virtual AP context 2-99

Interface context 2-118

VLAN interface context 2-120

RADIUS profiles context 2-122

IP QOS context 2-125

DHCP server context 2-127

GRE interface context 2-128

IPsec context 2-129

Syslog context 2-132
PPTP client interface 2-135
Keychain context 2-137
Keys context 2-138
Subscription plan context 2-139
SNMP user context 2-142
SNMP notification receiver context 2-143
Active Directory Group context 2-144
Controlled APs context 2-147
Controlled APs group context 2-149
Controlled APs base group context 2-150
Controlled APs network configuration context 2-151
Controlled APs VSC binding context 2-162
Syslog context 2-163
Provisioning connectivity context 2-165
Provisioning discovery context 2-168
Wireless interface context 2-170
RADIUS profile context 2-176
Local mesh profile context 2-177
Local mesh provisioning context 2-180
Switch port context 2-181
MAC addresses list context 2-186
Network profile context 2-187
LLDP agent context 2-188

View context

Path: View

This is the root of the command tree.

arping

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
arping [ -AbDfhqUV] [ -c <count>] [ -w <deadline>] [ -s <source>] -I <interface>
<destination>
```

Pings a destination on a device interface using ARP packets.

enable

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
enable
```

Switches to the enable context.

nslookup

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
nslookup [ -option authentication ] [ <host-to-find> | - [< server> ]]
```

Queries DNS servers for information on hosts or domains.

ping

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
ping <host> [-c <count>] [-s <length>] [-q]
```

Determines if the specified remote IP address is active.

Parameters

<-c host>	The IP address or DNS name of the host to ping.
<-c count>	Number of pings.
<-s length>	Length of the ping datagram.
<-q>	Quiet mode. No output.

ps

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
ps
```

Displays all running processes.

quit

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
quit
```

Quits the CLI.

show license

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
show license (eula | gpl | other)
```

Displays license information.

show logging filtered

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
show logging [filtered]
```

Displays the system log.

top

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
top
```

Displays all running processes.

traceroute

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
traceroute [-n] [-r] [-v] [-m <max_ttl>] [-p <port#>] [-q <nqueries>] [-s
<src_addr>] [-t <tos>] [-w <wait>] <host> [<data size>]
```

Displays the hosts that are traversed to reach the specified IP address.

Enable context

Path: View > Enable

This context provides access to various utilities.

reboot device

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
reboot device
```

Restarts the system.

show certificate

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
show certificate
```

Displays current certificates.

show certificate binding

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
show certificate binding
```

Displays how the certificates are used.

iperf

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
iperf -c host [-t time]
```

Runs a performance throughput test.

Parameters

<-c host>	The IP address or DNS name of the iperf server to connect to.
<-t length>	Length of the throughput test in seconds.

ping

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
ping <host> [-c <count>] [-s <length>] [-q]
```

Determines if the specified remote IP address is active.

Parameters

<-c host>	The IP address or DNS name of the host to ping.
<-c count>	Number of pings.
<-s length>	Length of the ping datagram.
<-q>	Quiet mode. No output.

arping

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
arping [ -AbDfhqUV] [ -c <count>] [ -w <deadline>] [ -s <source>] -I <interface>
<destination>
```

Pings a destination on a device interface using ARP packets.

arp

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
arp [-evn] [-H <type>] [-i if] ?- [<hostname>] arp [-v] [-i if] -d <hostname>
[pub] arp [-v] [-H <type>] [-i if] -s <hostname> <hw_addr> [temp] arp [-v] [-H
<type>] [-i if] -s <hostname> <hw_addr> [<netmask> <nm>] <pub> arp [-v] [-H
<type>] [-i if] -Ds <hostname> ifa [<netmask> <nm>] <pub>
```

Displays and modifies the Internet-to-Ethernet address translation tables used by the address resolution protocol.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
end
```

Switches to parent context.

quit

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
quit
```

Exits the enable context.

rcapture

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
rcapture -u <URI> [-c <count>] -i <interface>
```

Captures data on a port and sends it to a file on an FTP server.

Parameters

<URI>	Address of the FTP site and filename where the trace will be saved. For example: ftp://user:pass@ftp.mysite.com/trace.pcap
<count>	Number of packets to capture.
<interface>	Interface to trace: eth0 = Internet port, eth1 = LAN port, wvlan0 = wireless port

show arp

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
show arp
```

Displays the ARP table.

show bridge

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
show bridge
```

Displays bridge information.

show bridge forwarding

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
show bridge forwarding
```

Displays bridge forwarding information.

show dns cache

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
show dns cache [<serial>]
```

Displays DNS cache entries. Specify a serial number to display detailed information.

show interfaces

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
show interfaces
```

Displays networking interfaces.

show ip

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
show ip
```

Displays all IP addresses.

show ip route

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
show ip route
```

Displays all IP routes.

show system info

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
show system info
```

Displays basic system information.

show vsc overview

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
show vsc overview
```

Displays an overview of the current VSCs.

show controlled-aps wireless clients

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
show controlled-aps wireless clients
```

Displays all wireless clients associated with controlled APs.

disassociate controlled-ap wireless client _

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
disassociate controlled-ap wireless client [<client_macaddress>]
```

Terminates the connection for the specified wireless client.

show ip dhcp database

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
show ip dhcp database
```

Displays the DHCP server lease database.

show satellites

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
show satellites [<deviceid>]
```

Displays current satellites of this access point.

show web content

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
show web content
```

Displays all files inside the access points detected nearby.

show client log

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
show client log [<macaddr>]
```

Displays the client station log. Enter the MAC address to display more details for a specific client station.

show radius statistics

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
show radius statistics
```

Displays RADIUS server statistics.

show radius users

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
show radius users [<filter>]
```

Displays users that are using RADIUS accounting.

show users

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show users [<filter>]`

Displays all users on this controller.

show discrete pin

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show discrete pin`

Displays the state of the discrete pin.

config

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`config`

Switches to the config context.

show all config

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show all config`

Displays all configuration settings that apply to this device.

controlled network

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`controlled network (ap | group | base) [<name>] [<mac>]`

Creates or switches to the specified AP or group.

show controlled network config

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show controlled network config`

Displays configuration information for all controlled APs.

Config context

Path: View > Enable > Config

This is the root context for all configuration commands.

vlan

Supported on: E-MSM720

`vlan <networkname>`

Switches to the specified VLAN interface or create a new VLAN interface with the specified VLAN definition.

`no vlan <networkname>`

Deletes the specified VLAN.

New

interface

Supported on: E-MSM720

`interface <port>`

Switches to the specified physical interface (port).

dhcp public ip default lease period

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dhcp public ip default lease period <number>`

Defines the amount of time a public IP address lease will be valid.

dhcp public ip subnet

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dhcp public ip subnet`

Enables the DHCP server IP address pool to support the public IP address feature.

`no dhcp public ip subnet`

Disables DHCP server IP address pool support for the public IP address feature.

certificate

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`certificate (authority | local) <uri> <certname> [<password>]`

Adds a new certificate to the store, using the specified friendly name.

certificate binding

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`certificate binding (web-management | html-auth | soap | eap) <certname>`

Assigns a certificate to a service.

`no certificate binding (web-management | html-auth | soap | eap) <certname>`

Unassigns a certificate from a service.

certificate revocation

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`certificate revocation <uri> <certname>`

Adds a Certificate Revocation List (CRL) to an existing authority certificate.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`end`

Switches to parent context.

factory settings

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`factory settings`

Resets the system configuration to factory default settings.

network-profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`network-profile <name>`

Add/Edits the specified network profile or creates a new profile with the specified name.

`no network-profile <name>`

Deletes the network profile with the specified name.

reboot device

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`reboot device`

Restarts the system.

show certificate

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show certificate`

Displays current certificates.

show certificate binding

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show certificate binding`

Displays how the certificates are used.

show config factory

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
show config [factory]
```

Generates a list of CLI commands that can be used to define the currently loaded configuration.

show network-profiles

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
show network-profiles
```

Displays all currently defined network profiles.

show tech

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
show tech
```

Displays tech support information.

interface ethernet

Supported on: MSM710 MSM760 MSM765zl

```
interface ethernet (port-1|port-2)
```

Switches to the specified Ethernet interface context.

interface ip

Supported on: MSM710 MSM760 MSM765zl

```
interface ip (lan | wan)
```

Switches to the specified IP interface context.

interface pptp client-default

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
interface pptp client-default
```

Switches to the PPTP client interface context.

interface gre

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
interface gre <name>
```

Switches to the specified GRE interface or creates a new GRE interface with the specified name.

```
no interface gre <name>
```

Deletes the specified GRE interface.

New

show lacp

Supported on: E-MSM720

`show lacp`

Displays E-MSM720 LACP information.

New

show mac-address

Supported on: E-MSM720

`show mac-address [<port>]`

Displays the MAC forwarding table.

New

show mac-address count

Supported on: E-MSM720

`show mac-address count`

Displays the number of entries in the MAC forwarding table.

New

show trunks

Supported on: E-MSM720

`show trunks`

Displays trunking information.

New

show vlans

Supported on: E-MSM720

`show vlans`

Displays VLAN information.

virtual ap

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`virtual ap <name>`

Creates a new VSC (VAP) profile or switches to the existing VSC (VAP) context with the specified name.

`no virtual ap <name>`

Deletes the specified VSC (VAP) profile.

Parameters

name	Name of an existing or new VSC (VAP) profile.

cap-switch to

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`cap-switch to (ap | ac | wab)`

Switches to the specified operational mode.

Parameters

`ap`	Switches operational mode to CAP MultiService Access Point.
`ac`	Switches operational mode to CAP MultiService Controller.
`wab`	Switches operational mode to WAB Wireless Station.

show subscription plan

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show subscription plan [<name>]`

Displays one or more subscription plans.

subscription plan

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`subscription plan <name>`

Adds a new subscription plan.

`no subscription plan <name>`

Deletes the specified subscription plan.

mac list

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`mac list <name>`

Edits the specified MAC list or create a new list with the specified name.

`no mac list <name>`

Deletes the specified MAC list.

show mac list

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show mac list [<name>]`

Displays all current MAC lists, or details for the specified list.

ipsec policy

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ipsec policy <name>`

Switches to the specified IPSec policy or creates a new IPSec policy with the specified name.

admin local authentication

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`admin local authentication`

Sets the authentication of manager logins to occur using the local account.

`no admin local authentication`

Disables administrator authentication via the local account.

admin radius authentication

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`admin radius authentication`

Sets the authentication of manager logins to occur using RADIUS.

`no admin radius authentication`

Disables manager authentication via RADIUS.

admin radius authentication server

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`admin radius authentication server <name>`

Sets the authentication of manager logins to occur using RADIUS.

ip http port

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ip http port <number>`

Sets the port number to use for HTTP access to the controller.

Parameters

<number>	Port number. Range: 1 - 65535.

Description

HTTP connections made to this port are met with a warning and the browser is redirected to the secure web server port. By default. this parameter is set to port 80.

ip https port

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ip https port <number>`

Sets the port number used for HTTPS access to the controller.

Parameters

<number>	Port number. Range: 1 - 65535.

snmp-server trap certificate-expired

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snmp-server trap certificate-expired`

Send a trap when the SSL certificate has expired. A trap is sent every 12 hours.

`no snmp-server trap certificate-expired`

Do not send a trap when the SSL certificate has expired.

snmp-server trap certificate-expires-soon

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
snmp-server trap certificate-expires-soon
```

Send a trap when the SSL certificate is about to expire. A trap is sent every 12 hours starting 15 days before the certificate expires.

```
no snmp-server trap certificate-expires-soon
```

Do not send a trap when the SSL certificate is about to expire.

snmp-server trap web-fail

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
snmp-server trap web-fail
```

Send a trap each time an manager login is refused.

```
no snmp-server trap web-fail
```

Do not send a trap each time an manager login is refused.

snmp-server trap web-login

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
snmp-server trap web-login
```

Send a trap each time an manager login is accepted.

```
no snmp-server trap web-login
```

Do not send a trap each time an manager login is accepted.

snmp-server trap web-logout

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
snmp-server trap web-logout
```

Send a trap each time an manager logs out.

```
no snmp-server trap web-logout
```

Do not send a trap each time an manager logs out.

username

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
username <user> <password>
```

Changes the current manager local username and password.

Parameters

<user>	New manager username.
<password>	New manager password. New password must be between 6 and 16 printable characters in length and contain at least 4 different characters. Passwords are case sensitive. Space characters and double quotes cannot be used. Passwords must also conform to the Security policy that is in effect.

web admin kickout

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`web admin kickout`

Enables a new manager login to terminate an existing manager session.

`no web admin kickout`

Stops a new manager from logging in until an existing manager logs out.

web allow

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`web allow <ip address>/<mask>`

Adds an address to the list of hosts that can access the management tool.

`no web allow <ip address>/<mask>`

Removes the specified address from the list of hosts that can access the management tool.

Parameters

<address>	IP address.
</mask>	Subnet mask in CIDR format. Specifies the number of bits in the mask.

web access internet-port

Supported on: MSM710 MSM760 MSM765zl

`web access internet-port`

Enables access to the management tool via the Internet port.

`no web access internet-port`

Blocks access to the management tool via the Internet port.

web access lan-port

Supported on: MSM710 MSM760 MSM765zl

`web access lan-port`

Enables access to the management tool via the LAN port.

`no web access lan-port`

Blocks access to the management tool via the LAN port.

web access interface vlan

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`web access interface vlan <name>`

Enables access to the management tool via the specified VLAN.

`no web access interface vlan <name>`

Removes access to the management tool for the specified VLAN.

web access interface gre

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`web access interface gre <name>`

Enables access to the management tool via the specified GRE tunnel.

`no web access interface gre <name>`

Disables access to the management tool via the specified GRE tunnel.

web access vpn

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`web access vpn`

Enables access to the management tool via a VPN connection.

`no web access vpn`

Blocks access to the management tool via a VPN connection.

web access lan

Supported on: MSM710 MSM760 MSM765zl

`web access lan`

Enables access to the management tool via the LAN port.

`no web access lan`

Blocks access to the management tool via the LAN port.

dhcp mode

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dhcp mode (server | relay | none)`

Sets whether the controller operates as a DHCP server or DHCP relay agent.

enable console password reset

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`enable console password reset`

Enables Console Password Reset.

`no enable console password reset`

Disables Console Password Reset.

console authentication

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`console authentication (always-local | like-web)`

Sets how a CLI user gets authenticated.

dhcp server

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dhcp server lan`

Switches to the DHCP server context.

dhcp server default domain name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dhcp server default domain name <domain>`

Sets the DHCP server domain name.

dhcp server default lease period

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dhcp server default lease period <number>`

Sets the default lease time for the DHCP server.

dhcp server default permanent lease period

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dhcp server default permanent lease period <number>`

Sets the permanent lease time for the DHCP server.

dhcp server controller

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dhcp server controller <ip address>`

Add the specified IP address to the list of controllers.

`no dhcp server controller <ip address>`

Remove the specified IP address from the list of controllers.

Use the address list to define the IP address for one or more controllers that are active on the network. This list is sent to all devices that request an IP address, encoded as DHCP option 43 (Vendor-specific information). This option is only interpreted by HP APs that are operating in controlled mode. Controlled mode APs use these addresses to connect with the controllers in the order that they appear in the list.

dhcp server controller discovery

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dhcp server controller discovery`

Send the controller list, encoded as DHCP option 43, when assigning an address to a DHCP client.

`no dhcp server controller discovery`

Do not the controller address list to DHCP clients.

dhcp server logout html user

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dhcp server logout html user`

Logout HTML users upon discovery request.

`no dhcp server logout html user`

Do not logout HTML user upon discovery request.

The controller will log out a client station if a DHCP discovery request is received from the client station while a DHCP address lease is currently assigned. This feature is useful when multiple users share the same client station. If a user forgets to log out before turning off the client station, the next user will have to wait until the lease expires before being able to log in.

dhcp server access centralized clients

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dhcp server access centralized clients`

Listen for DHCP requests from access-controlled client stations using the client data tunnel.

`no dhcp server access centralized clients`

Do not listen for DHCP requests from access-controlled client stations using the client data tunnel.

dhcp server access lan

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dhcp server access lan`

Listen for DHCP request on the LAN port.

`no dhcp server access lan`

Do not listen for DHCP request on the LAN port.

dhcp relay

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dhcp relay <primary-ip-address> <[secondary-ip-address]>`

Sets the primary and secondary DHCP server for the relay.

dhcp relay circuit id

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dhcp relay circuit id <string>`

Sets the DHCP relay Option 82 circuit ID.

`no dhcp relay circuit id`

Clears the DHCP relay Option 82 circuit ID.

dhcp relay remote id

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dhcp relay remote id <string>`

Sets the DHCP relay Option 82 remote ID.

`no dhcp relay remote id`

Clears the DHCP relay Option 82 remote ID.

dhcp relay access centralized clients

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dhcp relay access centralized clients`

Listen for DHCP requests from access-controlled client stations using the client data tunnel.

`no dhcp relay access centralized clients`

Do not listen for DHCP requests from access-controlled client stations using the client data tunnel.

dhcp relay access lan

Supported on: MSM710 MSM760 MSM765zl

`dhcp relay access lan`

Listen for DHCP request on the LAN port.

`no dhcp relay access lan`

Do not listen for DHCP request on the LAN port.

New

dhcp relay access access network

Supported on: E-MSM720

`dhcp relay access access network`

Listen for DHCP request on the Access network.

`no dhcp relay access access network`

Do not listen for DHCP request on the Access network.

dhcp relay extend internet port

Supported on: MSM710 MSM760 MSM765zl

`dhcp relay extend internet port`

Alter DHCP requests so they appear to originate from the Internet port.

`no dhcp relay extend internet port`

Do not alter DHCP requests.

When enabled, the controller will alter the DHCP address requests from client stations so that they appear to originate from the network assigned to the Internet port on the controller. This will cause the DHCP server to assign IP addresses on this network to all client stations. The controller handles all mapping between the two subnets internally.

New

dhcp relay extend internet network

Supported on: E-MSM720

`dhcp relay extend internet network`

Alter DHCP requests so they appear to originate from the Internet network.

`no dhcp relay extend internet network`

Do not alter DHCP requests.

When enabled, the controller will alter the DHCP address requests from client stations so that they appear to originate from the network assigned to the Internet port on the controller. This will cause the DHCP server to assign IP addresses on this network to all client stations. The controller handles all mapping between the two subnets internally.

clock

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`clock <time> <date>`

Sets the system time and date.

Parameters

<time>	Time as hh:mm:ss. For example: 15:44:00.
<date>	Date as dd mmm yyyy. For example: 17 Oct 2004

clock auto adjust dst

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`clock auto adjust dst`

Automatically adjust clock for daylight savings changes.

`no clock auto adjust dst`

Do not automatically adjust clock for daylight savings changes.

clock timezone

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`clock timezone <gmtdiff>`

Sets the time zone the controller is operating in.

Parameters

<gmtdiff>	Offset from GMT as follows: +-HOUR:MIN. For example, Eastern Standard time is -5:00.

clock use custom dst rules

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`clock use custom dst rules`

Use custom DST rules instead of default ones.

`no clock use custom dst rules`

Do not use custom DST rules, use default ones.

ntp protocol

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
ntp protocol (ntp | sntp)
```

Sets the network time protocol to use.

ntp server

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
ntp server
```

Enable this option to have the controller periodically contact a network time server to update its internal clock.

```
no ntp server
```

Disables the use of a network time server.

clock custom dst begins

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
clock custom dst begins <day> <weekday> <month> <time>
```

Set parameters of the rule defining the beginning of daylight savings time.

Parameters

<day>	Day of the month. Range 1 - 31.
<weekday>	Weekday. Valid values are: "sun", "mon", "tue", "wed", "thu", "fri", "sat".
<month>	Month. Valid values are: "jan", "feb", "mar", "apr", "may", "jun", "jul", "aug", "sep", "oct", "nov", "dec".
<time>	Time as hh:mm[:ss]. For example: 15:44:00.

If a parameter does not apply to the configured DST rule format, simply set this parameter to any valid value.

clock custom dst begins format

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
clock custom dst begins format (<fixed>|<last-weekday>|<following-
date>|<preceding-date>
```

Set the format of the custom DST rule.

Parameters

<fixed>	Rule of the form: The [Day]th of [Month] at [Time].
<last-weekday>	Rule of the form: The last [Weekday] of [Month] at [Time].
<following-date>	Rule of the form: The first [Weekday] on or after the [Day]th of [Month] at [Time].
<preceding-date>	Rule of the form: The first [Weekday] on or before the [Day]th of [Month] at [Time].

clock custom dst ends

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`clock custom dst ends <day> <weekday> <month> <time>`

Set parameters of the rule defining the end of daylight savings time.

Parameters

<day>	Day of the month. Range 1 - 31.
<weekday>	Weekday. Valid values are: "sun", "mon", "tue", "wed", "thu", "fri", "sat".
<month>	Month. Valid values are: "jan", "feb", "mar", "apr", "may", "jun", "jul", "aug", "sep", "oct", "nov", "dec".
<time>	Time as hh:mm[:ss]. For example: 15:44:00.

If a parameter does not apply to the configured DST rule format, simply set this parameter to any valid value.

clock custom dst ends format

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`clock custom dst ends format (<fixed>|<last-weekday>|<following-date>|<preceding-date>`

Set the format of the custom DST rule.

Parameters

<fixed>	Rule of the form: The [Day]th of [Month] at [Time].
<last-weekday>	Rule of the form: The last [Weekday] of [Month] at [Time].
<following-date>	Rule of the form: The first [Weekday] on or after the [Day]th of [Month] at [Time].
<preceding-date>	Rule of the form: The first [Weekday] on or before the [Day]th of [Month] at [Time].

ntp server

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ntp server <index><host>`

Adds the specified network time server.

Parameters

<index>	Index of the time server in the list. Up to 20 time servers are supported. Time servers are checked in the order that they appear in the list.
<host>	DNS name or IP address of the time server.

ntp server failure trap

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ntp server failure trap`

Send a trap each time a time server synchronization failed.

`no ntp server failure trap`

Do not send a trap each time a time server synchronization failed.

config-update automatic

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`config-update automatic`

Enables scheduled configuration restore or backup.

`no config-update automatic`

Disables scheduled configuration restore or backup.

The controller can automatically download the configuration file from a local or remote URL (restore). It is also possible to upload the current configuration to a given URL (backup). Theses operations can be done at preset times.

config-update operation

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`config-update operation (restore | backup)`

Sets the type of operation that will take place at the preset time.

config-update start

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`config-update start`

Start a config update now. Will reboot on success.

config-update time

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`config-update time <time>`

Sets the time of day when the scheduled configuration operation (backup or restore) will take place.

Parameters

<time>	Time as hh:mm:ss. For example: 15:44:00.

config-update uri

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`config-update uri <uri>`

Sets the URI where the controller will download or upload the configuration file.

`no config-update uri`

Clears the configuration file URI.

config-update weekday

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`config-update weekday (everyday | monday | tuesday | wednesday | thursday | friday | saturday | sunday)`

Sets the day when the scheduled configuration operation (backup or restore) will take place.

snmp-server trap config-change

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snmp-server trap config-change`

Send a trap whenever the configuration is changed.

`no snmp-server trap config-change`

Do not send this trap.

snmp-server trap config-update

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snmp-server trap config-update`

Send a trap whenever the firmware is updated.

`no snmp-server trap config-update`

Do not send this trap.

logging destination

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`logging destination <name>`

Creates a new remote destination for syslog.

`no logging destination <name>`

Deletes the specified syslog destination.

Parameters

<name>	Name of syslog destination. Use the name "local" to edit your local log file settings. Any other name will edit/create a remote log destination.

snmp-server trap syslog-severity

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snmp-server trap syslog-severity`

Set the severity level of syslog messages that will trigger a trap.

`no snmp-server trap syslog-severity`

Do not send this trap.

snmp-server

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snmp-server`

Enables the SNMP agent.

`no snmp-server`

Disables the SNMP agent.

snmp-server allow

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snmp-server allow <ip address>/<mask>`

Adds a host to the list of IP address from which access to the SNMP interface is permitted.

`no snmp-server allow <ip address>/<mask>`

Removes a host from the list of IP address from which access to the SNMP interface is permitted.

Parameters

<address>	IP address.
</mask>	Subnet mask in CIDR format. Specifies the number of bits in the mask.

snmp-server chassis-id

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snmp-server chassis-id <name>`

Specifies a name to identify the controller. By default, this is set to the serial number of the controller.

`no snmp-server chassis-id`

Deletes the system name.

snmp-server contact

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snmp-server contact <email>`

Specifies contact information.

`no snmp-server contact`

Deletes contact information.

Parameters

<email>	Email address.

snmp-server heartbeat period

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snmp-server heartbeat period <seconds>`

Sets the interval between sending heartbeat traps.

Parameters

<seconds>	Heartbeat interval in seconds.

snmp-server location

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snmp-server location <name>`

Specifies the location where the controller is installed.

`no snmp-server location`

Deletes location information.

Parameters

<name>	Location where the controller is installed.

snmp-server port

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snmp-server port <port number>`

Sets the port the controller will use to respond to SNMP requests.

Parameters

<port number>	SNMP port number. Range 1 - 65535.

snmp-server readonly

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snmp-server readonly <community>`

Sets the read-only community string.

`no snmp-server readonly`

Deletes the read-only community string.

snmp-server readwrite

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snmp-server readwrite <community>`

Sets the read-write community string.

`no snmp-server readwrite`

Deletes the read-write community string.

snmp-server trap

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snmp-server trap`

Enables support for SNMP traps.

`no snmp-server trap`

Disables support for SNMP traps.

snmp-server trap community

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snmp-server trap community <str>`

Sets the password required by the remote host that will receive the trap.

`no snmp-server trap community`

Deletes the password required by the remote host that will receive the trap.

snmp-server trap destination

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snmp-server trap destination <host> <[port number]>`

Add a new trap destination.

`no snmp-server trap destination <host> [<port>]`

Deletes the specified trap destination.

Parameters

<host>	Sets the IP address or domain name of the host that the controller will send traps to.
<[port number]>	SNMP port number. Range 1 - 65535. By default port 162 is used

snmp-server trap heartbeat

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snmp-server trap heartbeat`

Enables sending of heartbeat traps at regular intervals.

`no snmp-server trap heartbeat`

Disables sending of heartbeat traps at regular intervals.

snmp-server trap link-state

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snmp-server trap link-state`

Send a trap when the link state changes on any interface.

`no snmp-server trap link-state`

Do not send this trap.

snmp-server trap snmp-authentication

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snmp-server trap snmp-authentication`

Send a trap each time an SNMP request fails to supply the correct community name.

`no snmp-server trap snmp-authentication`

Do not send a trap each time an SNMP request fails to supply the correct community name.

snmp-server version 1

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snmp-server version 1`

Enable support for SNMP version 1.

`no snmp-server version 1`

Disable support for SNMP version 1.

snmp-server version 2c

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snmp-server version 2c`

Enable support for SNMP version 2c.

`no snmp-server version 2c`

Disable support for SNMP version 2c.

snmp-server version 3

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snmp-server version 3`

Enable support for SNMP version 3.

`no snmp-server version 3`

Disable support for SNMP version 3.

snmp-server access interface vlan

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snmp-server access interface vlan <name>`

Enables access to SNMP via the specified VLAN.

`no snmp-server access interface vlan <name>`

Disables access to SNMP via the specified VLAN.

Parameters

<name>	Specifies the name of the VLAN.

snmp-server access interface gre

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snmp-server access interface gre <name>`

Enables access to SNMP via the specified GRE tunnel.

`no snmp-server access interface gre <name>`

Removes access to SNMP via the specified GRE tunnel.

snmp-server access port-1

Supported on: MSM710 MSM760 MSM765zl

`snmp-server access port-1`

Enables SNMP access on the downstream port.

`no snmp-server access port-1`

Blocks SNMP access on the downstream port.

snmp-server access port-2

Supported on: MSM710 MSM760 MSM765zl

```
snmp-server access port-2
```

Enables SNMP access on the upstream port.

```
no snmp-server access port-2
```

Blocks SNMP access on the upstream port.

snmp-server access vpn

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
snmp-server access vpn
```

Enables access to the management tool via a VPN connection.

```
no snmp-server access vpn
```

Blocks access to the management tool via a VPN connection.

snmp-server trap device-authorization-failure

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
snmp-server trap device-authorization-failure
```

Send a trap when the device is not authorized to connect to the service controller.

```
no snmp-server trap device-authorization-failure
```

Do not send a trap about device authorization failure.

snmp-server trap device-configuration-failure

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
snmp-server trap device-configuration-failure
```

Send a trap when the device does not accept a new configuration.

```
no snmp-server trap device-configuration-failure
```

Do not send a trap about device configuration failure.

snmp-server trap device-firmware-failure

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
snmp-server trap device-firmware-failure
```

Send a trap when the device does not accept a new firmware.

```
no snmp-server trap device-firmware-failure
```

Do not send a trap about device firmware failure.

snmp-server trap device-security-failure

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
snmp-server trap device-security-failure
```

Send a trap when the device is not able to establish a secure connection with the service controller.

```
no snmp-server trap device-security-failure
```

Do not send a trap about device security failure.

snmp-server trap device-state-change

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
snmp-server trap device-state-change
```

Send a trap when the device switch to a new state.

```
no snmp-server trap device-state-change
```

Do not send a trap about device state change.

snmp-server trap new-satellite-detected

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
snmp-server trap new-satellite-detected
```

Send a trap when a new satellite is detected.

```
no snmp-server trap new-satellite-detected
```

Do not send a trap when a new satellite is detected.

snmp-server trap satellite-unreachable

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
snmp-server trap satellite-unreachable
```

Send a trap when a satellite cannot be reached.

```
no snmp-server trap satellite-unreachable
```

Ignore unreachable satellites.

snmp-server trap service-controller-state

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
snmp-server trap service-controller-state
```

Send a trap when a service controller leave or enter the runnig state.

```
no snmp-server trap service-controller-state
```

Do not send a trap about service controller states.

snmp-server access lan

Supported on: MSM710 MSM760 MSM765zl

`snmp-server access lan`

Enables access to the management tool via the LAN port.

`no snmp-server access lan`

Blocks access to the management tool via the LAN port.

snmp-server user

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snmp-server user <name>`

Creates a new SNMP user or switches to the SNMP user context with the specified user name.

`no snmp-server user <name>`

Deletes the specified SNMP user.

snmp-server notification receiver

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snmp-server notification receiver <host>`

Creates a new SNMP notification receiver or switches to the SNMP notification receiver context with the specified IP address.

`no snmp-server notification receiver <host>`

Deletes the specified SNMP notification receiver.

soap-server

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`soap-server`

Enables the SOAP server.

`no soap-server`

Disables the SOAP server.

soap-server access interface vlan

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`soap-server access interface vlan <name>`

Enables access to SOAP via this VLAN.

`no soap-server access interface vlan <name>`

Disables access to SOAP via this VLAN.

soap-server allow

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`soap-server allow <ip address>/<mask>`

Adds a host to the list of IP addresses from which access to the SOAP interface is permitted.

`no soap-server allow <ip address>/<mask>`

Removes a host from the list of IP addresses from which access to the SOAP interface is permitted.

Parameters

<address>	IP address.
</mask>	Subnet mask in CIDR format. Specifies the number of bits in the mask.

soap-server http authentication

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`soap-server http authentication`

Enable the SOAP server HTTP authentication.

`no soap-server http authentication`

Disable the SOAP server HTTP authentication.

soap-server http authentication password

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`soap-server http authentication password`

Set the SOAP server HTTP authentication password.

soap-server http authentication username

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`soap-server http authentication username`

Set the SOAP server HTTP authentication username.

soap-server port

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`soap-server port <port number>`

Sets the port the controller will use to respond to SOAP requests.

Parameters

<port number>	SOAP port number. Range 1 - 65535.

soap-server ssl

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`soap-server ssl`

SSL enabled for SOAP server.

```
no soap-server ssl
```

SSL disabled for SOAP server.

soap-server ssl with client certificate

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
soap-server ssl with client certificate
```

Enable the use of client certificate with SSL for SOAP server.

```
no soap-server ssl with client certificate
```

Disable the use of client certificate with SSL for SOAP server.

soap-server access interface gre

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
soap-server access interface gre <name>
```

Enables access to SOAP via the specified GRE tunnel.

```
no soap-server access interface gre <name>
```

Removes access to SOAP via the specified GRE tunnel.

soap-server access port-1

Supported on: MSM710 MSM760 MSM765zl

```
soap-server access port-1
```

Enables SOAP access on the downstream port.

```
no soap-server access port-1
```

Blocks SOAP access on the downstream port.

soap-server access port-2

Supported on: MSM710 MSM760 MSM765zl

```
soap-server access port-2
```

Enables SOAP access on the upstream port.

```
no soap-server access port-2
```

Blocks SOAP access on the upstream port.

soap-server access lan

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
soap-server access lan
```

Enables access to the management tool via the LAN port.

```
no soap-server access lan
```

Blocks access to the management tool via the LAN port.

soap-server access vpn

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
soap-server access vpn
```

Enables access to the management tool via a VPN connection.

```
no soap-server access vpn
```

Blocks access to the management tool via a VPN connection.

snmp-server trap vpn-connection

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
snmp-server trap vpn-connection
```

Send a trap when a user establishes a VPN connection with the controller.

```
no snmp-server trap vpn-connection
```

Do not send this trap.

snmp-server trap syslog-matches

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
snmp-server trap syslog-matches
```

Send a trap when syslog messages matches a specified regular expression.

```
no snmp-server trap syslog-matches
```

Do not send this trap.

snmp-server trap syslog-matches regex

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
snmp-server trap syslog-matches regex <regex>
```

Sets the regular expression used to match the syslog messages.

snmp-server trap syslog-severity level

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
snmp-server trap syslog-severity level (debug | info | notice | warning | error
| critical | alert | emergency)
```

Set the severity level of syslog messages that will trigger a trap.

snmp-server trap network-trace

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
snmp-server trap network-trace
```

Send a trap when a network trace is started or stopped.

```
no snmp-server trap network-trace
```

Do not send this trap.

firmware-update automatic

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`firmware-update automatic`

Enables scheduled firmware upgrades.

`no firmware-update automatic`

Disables scheduled firmware upgrade.

The controller can automatically retrieve and install firmware from a local or remote URL at preset times. By placing controller firmware on a web or ftp server, you can automate the update process for multiple units.

When the update process is triggered the controller retrieves the first 2K of the firmware file to determine if it is different from the active version. If different, the entire firmware file is then downloaded and installed.

(Different means older or newer. This enables you to return to a previous firmware version if required).

Configuration settings are preserved during the update unless stated otherwise in the release notes for the firmware. However, all active connections will be terminated. Customers will have to log in again after the controller restarts

firmware-update start

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`firmware-update start`

Upload the firmware based on a specified URI. This URI can be set with the command: firmware-update uri.

firmware-update time

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`firmware-update time <time>`

Sets the time of day the scheduled firmware upgrade will take place.

Parameters

<time>	Time as hh:mm:ss. For example: 15:44:00.

firmware-update uri

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`firmware-update uri <uri>`

Sets the URI where the controller will retrieve new firmware.

`no firmware-update uri`

Clears the firmware URI.

firmware-update weekday

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
firmware-update weekday (everyday | monday | tuesday | wednesday | thursday |
friday | saturday | sunday)
```

Sets the day when the scheduled firmware upgrade will take place.

snmp-server trap firmware-update

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
snmp-server trap firmware-update
```

Send a trap on firmware update.

```
no snmp-server trap firmware-update
```

Do not send a trap on firmware update.

ip name-server

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
ip name-server <primary> [<secondary>] [<third>]
```

Sets the primary and secondary DNS servers overriding dynamically assigned ones.

Parameters

<primary>	IP address of the primary DNS server.
<secondary>	IP address of the secondary DNS server.
<third>	IP address of the third DNS server.

ip name-server cache

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
ip name-server cache
```

Enables the DNS cache.

```
no ip name-server cache
```

Disables the DNS cache.

Once a host name has been successfully resolved to an IP address by a remote DNS server, it is stored in the cache. This speeds up network performance, as the remote DNS server now does not have to be queried for subsequent requests for this host.

The entry stays in the cache until:

- an error occurs when connecting to the remote host
- the time to live (TTL) of the DNS request expires
- the controller is restarted

ip name-server dynamic

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
ip name-server dynamic
```

Enables dynamic assignment of DNS servers.

`no ip name-server dynamic`

Disables dynamic DNS assignment.

ip name-server interception

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ip name-server interception`

Intercept all DNS requests from users and relay them to configured servers.

`no ip name-server interception`

Process DNS requests addressed to this device only.

ip name-server switch-on-servfail

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ip name-server switch-on-servfail`

Switch to next server when server failure is received.

`no ip name-server switch-on-servfail`

Do not switch to next server when server failure is received.

ip name-server switch-over

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ip name-server switch-over`

Switch over to primary when active.

`no ip name-server switch-over`

Do not switch over to primary when active.

ip name-server logout-info

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ip name-server logout-info <host> <ip address>`

Sets the logout host name and the logout IP address.

access controller shared secret

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`access controller shared secret <secret>`

Sets the shared secret used to communicate with the controller.

`no access controller shared secret`

Sets the shared secret used to communicate with the access controller.

The controller will only accept authentication/location-aware information from HP APs that have a matching shared secret to its own.

radius-server profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius-server profile <name>`

Creates a new RADIUS profile or switches to the RADIUS context with the specified profile name.

`no radius-server profile <name>`

Deletes the specified RADIUS profile.

ip-qos profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ip-qos profile <name>`

Creates a new IP QoS profile or switches to the IP QoS context with the specified profile name.

`no ip-qos profile <name>`

Deletes the specified IP QoS profile.

access controller

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`access controller`

Switches to the access controller context.

certificate ipsec ca

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`certificate ipsec ca <uri>`

Loads a new CA certificate from the specified URI.

The URI can be local:

- local://FILENAME

or remote

- ftp://host/path

certificate ipsec local

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`certificate ipsec local <uri> <password>`

Loads a new local certificate from the specified URI.

`no certificate ipsec local`

Removes the local certificate.

The URI can be local:

- local://FILENAME

or remote

- ftp://host/path

certificate ipsec revocation

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`certificate ipsec revocation <uri>`

Loads a new CRL file from the specified URI.

The URI can be local:

- local://FILENAME

or remote

- ftp://host/path

certificate ssl

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`certificate ssl <uri> <password>`

Loads a new SSL certificate using the URI.

session profile default

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`session profile default`

Switches to the session profile context.

session profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`session profile <name>`

Switches to the session profile context.

`no session profile <name>`

Removes the specified session profile.

show session profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show session profile`

Display all session profiles.

remote configuration

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`remote configuration (radius)`

Switches to the RADIUS remote configuration context.

lldp config

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`lldp config <port>`

Edit LLPD port specific options.

lldp dynamic-name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`lldp dynamic-name`

Enables the LLDP dynamic naming feature.

`no lldp dynamic-name`

Disables the LLDP dynamic naming feature.

lldp dynamic-name refresh-time

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`lldp dynamic-name refresh-time <time>`

Sets the interval at which dynamic names for controlled APs are updated.

lldp dynamic-name user-string

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`lldp dynamic-name user-string <name>`

Specifies the text to use for the dynamic name.

You can use regular text in combination with placeholders to create the name. Placeholders are automatically expanded each time the name is regenerated.

Placeholders

`%RN`	System name of the neighboring device to which the port is connected, obtained via the System Name TLV. Since this is an optional TLV, if it is not available, the Chassis ID TLV is used instead.
`%RP`	Port description of the port on the neighboring device to which the local port is connected, obtained via the Port Description TLV. Since this is an optional TLV, if it is not available, the Port ID TLV is used instead.
`%SN`	Controller's serial number.
`%IP`	Controller's IP address. An IP address can require up to 15 characters (nnn.nnn.nnn.nnn).

lldp fast-start-count

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`lldp fast-start-count <count>`

After an MED LLDPDU is received, this timer is started and the agent sends one MED LLDPDU to the MED device each second as it counts down.

lldp holdtime-multiplier

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`lldp holdtime-multiplier <hold>`

Sets the hold time multiplier for LLDPDU transmissions.

The value of Multiplier is multiplied by the refresh-interval to define Time to live. Time to live indicates the length of time that neighbors will consider LLDP information sent by this agent to be valid.

lldp med-location civic-address-element

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`lldp med-location civic-address-element <caelement>`

Adds a Civic Address Element.

lldp med-location elin-addr

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`lldp med-location elin-addr <elin>`

Sets the Emergency Call Services ELIN as described, for example, by NENA TID 07-501.

lldp refresh-interval

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`lldp refresh-interval <time>`

Sets the interval (in seconds) at which local LLDP information is updated and TLVs are sent to neighboring network devices.

lldp run

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`lldp run`

Enables the LLDP Agent.

`no lldp run`

Disables the LLDP Agent.

show lldp config

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show lldp config [<port>]`

Displays LLDP configuration settings.

show lldp info local-device

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show lldp info local-device [<port>]`

Displays LLDP configuration settings.

show lldp info remote-device

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show lldp info remote-device [<port>]`

Displays LLDP configuration settings.

show lldp stats

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show lldp stats [<port>]`

Displays LLDP statistics for all ports or a specific port .

discovery protocol

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`discovery protocol`

Enables broadcast of HP device information for interoperability with CDP-enabled networking hardware.

`no discovery protocol`

Disables broadcast of HP device information.

discovery protocol device-id

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`discovery protocol device-id <name>`

Overwrite the device-id field of information packets (the controller serial number is not used).

`no discovery protocol device-id`

Do not overwrite the device-id field of information packets (use the controller serial number).

service controller ap authentication credentials

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`service controller ap authentication credentials <username> <password>`

When the RADIUS authentication source is selected, this option specifies the RADIUS username and password assigned to the controller.

`no service controller ap authentication credentials`

Clears the RADIUS username/password.

service controller ap authentication enable

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`service controller ap authentication enable`

Enables authentication of discovered controlled APs.

`no service controller ap authentication enable`

Disables AP authentication.

service controller ap authentication file

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`service controller ap authentication file <name>`

Sets the file to use for authentication of controlled access points. This must be an ASCII file with one or more MAC addresses in it. Each address must appear on a separate line.

service controller ap authentication radius-server

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`service controller ap authentication radius-server <name>`

Sets the RADIUS profile to use for authentication of controlled access points.

service controller ap authentication refresh-rate

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`service controller ap authentication refresh-rate <number>`

Specifies the interval at which the controller retrieves authentication list entries from the selected authentication source(s).

service controller ap authentication source file

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`service controller ap authentication source file`

Enables the use of a file authentication source.

`no service controller ap authentication source file`

Disables the use of a file authentication source.

service controller ap authentication source local

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`service controller ap authentication source local`

Enables the use of local authentication source.

`no service controller ap authentication source local`

Disables the use of local authentication source.

service controller ap authentication source radius

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`service controller ap authentication source radius`

Enables the use of RADIUS authentication source.

`no service controller ap authentication source radius`

Disables the use of RADIUS authentication source.

service controller discovery

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`service controller discovery`

Enable controller discovery.

`no service controller discovery`

Disable service controller discovery.

service controller primary

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`service controller primary`

Become the Primary controller.

`no service controller primary`

Become a secondary controller.

service controller primary ip addr

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`service controller primary ip addr <ip address>`

Configure a static ip address for the primary controller.

service controller priority

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`service controller priority <number>`

Sets this device's discovery priority.

service controller discovery interface internet-port

Supported on: MSM710 MSM760 MSM765zl

`service controller discovery interface internet-port`

Allow discovery on the LAN port.

`no service controller discovery interface internet-port`

Allow discovery on the LAN port.

service controller discovery interface lan-port

Supported on: MSM710 MSM760 MSM765zl

`service controller discovery interface lan-port`

Allow discovery on the LAN port.

`no service controller discovery interface lan-port`

Allow discovery on the LAN port.

New

service controller discovery interface

Supported on: E-MSM720

`service controller discovery interface <interface>`

Allow discovery on the specified interface.

`no service controller discovery interface <interface>`

Denies discovery on the specified interface.

service controller provisioning

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`service controller provisioning`

Enable the AP provisioning system.

`no service controller provisioning`

Disable the AP provisioning system.

bandwidth control internet-port

Supported on: MSM710 MSM760 MSM765zl

`bandwidth control internet-port`

Enables bandwidth control on the Internet port.

`no bandwidth control internet-port`

Disables bandwidth control on the Internet port.

bandwidth control internet-port high

Supported on: MSM710 MSM760 MSM765zl

`bandwidth control internet-port high <min-tx-%> <min-rx-%> <max-tx-%> <max-rx-%>`

Sets the bandwidth rates (Tx minimum, Tx maximum, Rx minimum, and Rx maximum) for traffic classed as High.

bandwidth control internet-port low

Supported on: MSM710 MSM760 MSM765zl

`bandwidth control internet-port low <min-tx-%> <min-rx-%> <max-tx-%> <max-rx-%>`

Sets the bandwidth rates (Tx minimum, Tx maximum, Rx minimum, and Rx maximum) for traffic classed as Low.

bandwidth control internet-port max-rate

Supported on: MSM710 MSM760 MSM765zl

`bandwidth control internet-port max-rate<transmit>)<receive>)`

Sets the maximum transmit and receive rates on the Internet port in kbps.

These settings enable you to limit the total incoming or outgoing data rate on the Internet port. If traffic exceeds the rate you set for short bursts, it is buffered. Long overages will result in data being dropped. To utilize the full available bandwidth, the transmit and receive limits should be set to match the incoming and outgoing data rates on the Internet port.

Parameters

<transmit>	Sets the maximum transmit rate in kbps.
<receive>	Sets the maximum receive rate in kbps.

About bandwidth control

Bandwidth rates for each level are defined by taking a percentage of the maximum transmit and receive rates defined for the Internet port. Each bandwidth level has four rate settings:

- Transmit rate - guaranteed minimum: This is the minimum amount of bandwidth that will be assigned to a level as soon as outgoing traffic is present on the level.
- Transmit rate - maximum: This is the maximum amount of outgoing bandwidth that can be consumed by the level. Traffic in excess will be buffered for short bursts, and dropped for sustained overages.
- Receive rate - guaranteed minimum: This is the minimum amount of bandwidth that will be assigned to a level as soon as incoming traffic is present on the level.
- Receive rate - maximum: This is the maximum amount of incoming bandwidth that can be consumed by the level. Traffic in excess will be buffered for short bursts, and dropped for sustained overages.

Bandwidth levels are arranged in order of priority from Very High to Low. Priority determines how free bandwidth is allocated once the minimum rate has been met for each level. Free bandwidth is always assigned to the higher priority levels first.

Assigning traffic to bandwidth levels

- Customer traffic is assigned to a bandwidth level on a per-VAP (VSC) basis.
- Management traffic (RADIUS, SNMP, management tool admin sessions) is assigned to bandwidth level Very High and cannot be changed.
- All traffic assigned to a particular bandwidth level shares the allocated bandwidth for that level.

bandwidth control internet-port normal

Supported on: MSM710 MSM760 MSM765zl

`bandwidth control internet-port normal <min-tx-%> <min-rx-%> <max-tx-%> <max-rx-%>`

Sets the bandwidth rates (Tx minimum, Tx maximum, Rx minimum, and Rx maximum) for traffic classed as Normal.

bandwidth control internet-port very-high

Supported on: MSM710 MSM760 MSM765zl

`bandwidth control internet-port very-high <min-tx-%> <min-rx-%> <max-tx-%> <max-rx-%>`

Sets the bandwidth rates (Tx minimum, Tx maximum, Rx minimum, and Rx maximum) for traffic classed as Very High.

New

bandwidth control

Supported on: E-MSM720

`bandwidth control`

Enables bandwidth control for traffic going between the Access and the Internet network.

`no bandwidth control`

Disables bandwidth control for traffic going between the Access and the Internet network.

New

bandwidth control high

Supported on: E-MSM720

`bandwidth control high <min-tx-%> <min-rx-%> <max-tx-%> <max-rx-%>`

Sets the bandwidth rates (Tx minimum, Tx maximum, Rx minimum, and Rx maximum) for traffic classed as High.

New

bandwidth control low

Supported on: E-MSM720

`bandwidth control low <min-tx-%> <min-rx-%> <max-tx-%> <max-rx-%>`

Sets the bandwidth rates (Tx minimum, Tx maximum, Rx minimum, and Rx maximum) for traffic classed as Low.

New

bandwidth control max-rate

Supported on: E-MSM720

`bandwidth control max-rate<transmit>)<receive>)`

Sets the maximum transmit and receive rates in kbps.

These settings enable you to limit the total incoming or outgoing data rate on the Internet network. If traffic exceeds the rate you set for short bursts, it is buffered. Long overages will result in data being dropped. To utilize the full available bandwidth, the transmit and receive limits should be set to match the incoming and outgoing data rates on the Internet network.

Parameters

<transmit>	Sets the maximum transmit rate in kbps.
<receive>	Sets the maximum receive rate in kbps.

About bandwidth control

Bandwidth rates for each level are defined by taking a percentage of the maximum transmit and receive rates defined for the Internet network. Each bandwidth level has four rate settings:

- Transmit rate - guaranteed minimum: This is the minimum amount of bandwidth that will be assigned to a level as soon as outgoing traffic is present on the level.
- Transmit rate - maximum: This is the maximum amount of outgoing bandwidth that can be consumed by the level. Traffic in excess will be buffered for short bursts, and dropped for sustained overages.
- Receive rate - guaranteed minimum: This is the minimum amount of bandwidth that will be assigned to a level as soon as incoming traffic is present on the level.

- Receive rate - maximum: This is the maximum amount of incoming bandwidth that can be consumed by the level. Traffic in excess will be buffered for short bursts, and dropped for sustained overages.

Bandwidth levels are arranged in order of priority from Very High to Low. Priority determines how free bandwidth is allocated once the minimum rate has been met for each level. Free bandwidth is always assigned to the higher priority levels first.

Assigning traffic to bandwidth levels

- Customer traffic is assigned to a bandwidth level on a per-VAP (VSC) basis.
- Management traffic (RADIUS, SNMP, management tool admin sessions) is assigned to bandwidth level Very High and cannot be changed.
- All traffic assigned to a particular bandwidth level shares the allocated bandwidth for that level.

New

bandwidth control normal

Supported on: E-MSM720

`bandwidth control normal <min-tx-%> <min-rx-%> <max-tx-%> <max-rx-%>`

Sets the bandwidth rates (Tx minimum, Tx maximum, Rx minimum, and Rx maximum) for traffic classed as Normal.

New

bandwidth control very-high

Supported on: E-MSM720

`bandwidth control very-high <min-tx-%> <min-rx-%> <max-tx-%> <max-rx-%>`

Sets the bandwidth rates (Tx minimum, Tx maximum, Rx minimum, and Rx maximum) for traffic classed as Very High.

ip route gateway

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ip route gateway<destination>/<mask> <gateway> <[metric]>`

Adds a static route.

`no ip route gateway <destination>/<mask> <gateway> <[metric]>`

Removes the specified static route.

Parameters

<destination>	Traffic addressed to this IP address will be routed.
<mask>	Indicates the number of bits in the destination address that is checked for a match.
<gateway>	Indicates the IP address of the gateway the controller will forward routed traffic to. The gateway address must be on the same subnet as one of the available interfaces (Internet port or LAN port).
<metrix>	Indicates the priority of a route. If two routes exist for a destination address then the controller chooses the one with the lower metric.

firewall mode

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`firewall mode (high|low|none)`

Sets the firewall mode.

Parameters

`high`	Permits all outgoing traffic. Blocks all externally initiated connections.
`low`	Permits all incoming and outgoing traffic, except for NetBIOS traffic. Use this option if you require active FTP sessions.
`none`	Disables the firewall.

show user profiles

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show user profiles [<pattern>]`

Display current local users.

show user profiles details

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show user profiles details <name>`

Display detailed information about the specified user.

user profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`user profile <name>`

Adds or edits the specified username in the local user list.

`no user profile <name>`

Removes the specified username from the local user list.

renew user profile subscription

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`renew user profile subscription [<username>]`

Renew the specified user with their assigned subscription plan.

New

dot1x radius accounting start delay

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`802.1x RADIUS accounting start delay <seconds>`

Sets the 802.1X RADIUS accounting start delay.

Parameters

<seconds>	delay in seconds.

dot1x reauth

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
dot1x reauth
```

Enable this option to force 802.1X client stations to reauthenticate.

```
no dot1x reauth
```

Disables 802.1X reauthentication.

dot1x reauth period

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
dot1x reauth period (15m | 30m | 1h | 2h | 4h | 8h | 12h)
```

Sets the 802.1X reauthentication interval. Client stations must reauthenticate when this interval expires.

dot1x reauth terminate

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
dot1x reauth terminate
```

Enable this option to allow client stations to remain connected during re-authentication. Client traffic is blocked only when re-authentication fails.

```
no dot1x reauth terminate
```

Disabled this option to block client traffic during re-authentication and only activate traffic again if authentication succeeds.

dot1x supplicant timeout

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
dot1x supplicant timeout <number>
```

Sets the 802.1X supplicant time-out.

Parameters

<seconds>	time-out in seconds.

dynamic key

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
dynamic key
```

Enables dynamic key support for 802.1X and WPA.

```
no dynamic key
```

Disables dynamic key support for 802.1X and WPA.

dynamic key interval

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dynamic key interval (5m | 10m | 15m | 30m | 1h | 2h | 4h | 8h | 12h)`

Specifies how often (in minutes or hours) that the group (broadcast) key is changed for 802.1X and WPA.

key chain

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`key chain <name>`

Switch to the specified key chain or create a new key chain.

`no key chain <name>`

Remove the specified key chain.

config-version

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`config-version <string>`

Sets a string to identify the user configuration version.

radius-server accounting session

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius-server accounting session <number>`

Set the maximum number of accounting sessions.

radius-server client

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius-server client`

Enable radius clients list.

`no radius-server client`

Disable radius clients list.

radius-server local eap-peap

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius-server local eap-peap`

Allow EAP-PEAP.

`no radius-server local eap-peap`

Disallow EAP-PEAP.

radius-server local eap-tls

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius-server local eap-tls`

Allow EAP-TLS.

`no radius-server local eap-tls`

Disallow EAP-TLS.

radius-server local eap-ttls

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius-server local eap-ttls`

Allow EAP-TTLS.

`no radius-server local eap-ttls`

Disallow EAP-TTLS.

radius-server local pap

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius-server local pap`

Allow PAP.

`no radius-server local pap`

Disallow PAP.

radius-server ssid detection nas-id

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius-server ssid detection nas-id`

Use NAS-ID for SSID detection.

`no radius-server ssid detection nas-id`

Do not use NAS-ID for SSID detection.

show radius-server

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show radius-server`

Displays the current RADIUS server configuration.

active-directory check attribute

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`active-directory check attribute <ldapattr>`

Sets the name of the Active Directory attribute to check for.

`no active-directory check attribute`

Remove the name of the Active Directory attribute.

active-directory check user access

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`active-directory check user access`

Check Active Directory for user access.

`no active-directory check user access`

Do not check Active Directory for user access.

active-directory device name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`active-directory device name <name>`

Sets the device NetBIOS name.

`no active-directory device name`

Removes the device NetBIOS name.

active-directory domain

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`active-directory domain <domain>`

Sets the Active Directory Windows domain.

`no active-directory domain`

Resets the Active Directory Windows domain.

active-directory domain netbios name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`active-directory domain netbios name <name>`

Set the Domain NetBIOS name.

`no active-directory domain netbios name`

Unset the Domain NetBIOS name.

active-directory group

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`active-directory group <name>`

Creates or goes to an Active Directory group.

`no active-directory group <name>`

Removes an Active Directory group.

active-directory group order

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`active-directory group order <number> <name>`

Reorders an Active Directory group.

active-directory join

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`active-directory join <username> <password>`

Joins with Active Directory.

show active-directory

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show active-directory`

Displays Active Directory settings.

show active-directory group

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show active-directory group <name>`

Displays details about an Active Directory group.

radius-server client

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius-server client <ip address>/<mask> <secret>`

Add a new radius client.

`no radius-server client <ip address>/<mask>`

Deletes an existing RADIUS client.

user tracking

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`user tracking`

Enables capture of usage data.

`no user tracking`

Disables capture of usage data.

user tracking destination

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`user tracking destination <host>`

Specifies the destination where the syslog packets should be sent.

user tracking filter

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`user tracking filter <filter>`

A comma-separated list of filters (username or subnet).

user tracking port

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`user tracking port <number>`

Specifies where UDP port capture data should be sent.

persistent user information

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`persistent user information`

Save user account information locally.

`no persistent user information`

Do not save user account information locally.

persistent user information period

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`persistent user information period <number>`

Period, in minutes, at which to update user information.

client data tunnel security

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`client data tunnel security (hmac | key)`

Specifies the security strength of the client data tunnel.

igmp proxy

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`igmp proxy`

Enables IGMP proxy.

`no igmp proxy`

Disables IGMP proxy.

igmp proxy downstream interface

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`igmp proxy downstream interface <interface>`

Sets the downstream IGMP port.

igmp proxy upstream interface

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`igmp proxy upstream interface <interface>`

Sets the upstream IGMP port.

rf-id aeroscout

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`rf-id aeroscout`

Enables AeroScout tag processing.

`no rf-id aeroscout`

Disables AeroScout tag processing.

sflow

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`sflow`

Enables sFlow.

`no sflow`

Disables sFlow.

show sflow agent

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show sflow agent`

Displays read-only sFlow agent information.

show sflow controller stats

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show sflow controller stats`

Displays read-only sFlow controller statistics.

show sflow device stats

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show sflow device stats <macaddress>`

Displays read-only sFlow device statistics.

sflow destination 80211

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`sflow <receiver> destination <ipaddress> [<port>] [<80211toethernet>]`

Sets the IP address of an sFlow collector/management station.

show sflow destination

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show sflow <receiver> destination`

Shows sFlow receiver configuration.

show sflow sampling-polling

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show sflow <receiver> sampling-polling [<interface>]`

Shows sFlow sampling and polling configuration for a receiver.

sflow sampling

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`sflow <receiver> sampling <interface> <rate>`

Specifies the number of packets between samples. For example, if set to 5, every fifth packet will be sampled. 0 disables sampling.

sflow polling

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`sflow <receiver> polling <interface> <interval>`

Specifies the maximum interval (seconds) between polling of counters. 0 disables polling.

sflow interface

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`sflow interface <ifindex>`

Makes the given sFlow interface visible to sFlow collectors.

`no sflow interface <ifindex>`

Makes the given interface invisible to sFlow collectors.

mac lockout entry

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`mac lockout entry <mac>`

Adds a new entry to the MAC lockout list.

`no mac lockout entry <mac>`

Removes the entry from the MAC lockout list.

show mac lockout

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show mac lockout`

Displays all entries in the MAC lockout list.

New

team communication ip address

Supported on: E-MSM720 MSM760 MSM765zl

`team communication ip address <ip address>/<mask>`

Sets the team communcation VLAN IP Address.

New

team communication vlan

Supported on: E-MSM720 MSM760 MSM765zl

`team communication vlan <id>`

Sets the team communcation VLAN ID.

`no team communication vlan`

Disables usage of a VLAN for team communication.

team management address

Supported on: E-MSM720 MSM760 MSM765zl

`team management address <ip address>/<mask>`

Sets the IP address that will be used to manage the team.

team manager

Supported on: E-MSM720 MSM760 MSM765zl

`team manager`

Sets this controller as the team manager. Only one team manager can be defined per team.

`no team manager`

Removes this controller as the team manager.

New

team name

Supported on: E-MSM720 MSM760 MSM765zl

`team name <name>`

Sets the team name.

teaming

Supported on: E-MSM720 MSM760 MSM765zl

`teaming`

Enables controller teaming.

New

team communication interface

Supported on: MSM760 MSM765zl

`team communication interface (internet | lan)`

Sets the port to use for communication with the team manager.

New

team communication interface

Supported on: E-MSM720

`team communication interface [<port>]`

Sets the port to use for communication with the team manager.

New

team communication vlan

Supported on: MSM760 MSM765zl

`team communication vlan`

Enables the use of a VLAN for team communication.

`no team communication vlan`

Disables usage of a VLAN for team communication.

team management interface

Supported on: MSM760 MSM765zl

`team management interface (internet | lan | vlan) [<name>]`

Sets the interface on which the team IP address will be active.

team management interface vlan

Supported on: E-MSM720

`team management interface vlan <name>`

Sets the interface on which the team IP address will be active.

Access Controller context

Path: View > Enable > Config > Access Controller

Use this context to define all global controller configuration settings.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
end
```

Switches to parent context.

ads presentation

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
ads presentation
```

Enables advertisement display at regular intervals for authenticated users.

```
no ads presentation
```

Disables advertisement display for authenticated users.

ads presentation interval

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
ads presentation interval <number>
```

Controls the advertisement display interval.

station free access

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
station free access
```

When enabled, all users are automatically granted access when the RADIUS server is down or unreachable.

```
no station free access
```

Customers cannot connect when the RADIUS server is unreachable.

Once the RADIUS server is available again, free user sessions remain active until the user logs out. This does not apply to users using 802.1X or WPA.

station http proxy html authentication only support

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
station http proxy html authentication only support
```

Restricts HTTP proxy support to HTML-based authenticated users only.

```
no station http proxy html authentication only support
```

Allows HTTP proxy support for other authenticated users as well.

station http proxy support

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
station http proxy support
```

Enables support for client stations that are configured to use a proxy server for HTTP and HTTPS, without requiring users to reconfigure their systems.

```
no station http proxy support
```

Disables support for client stations that are configured to use a proxy server for HTTP and HTTPS.

station idle detection

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
station Idle detection <interval> <count>
```

The controller continuously polls authenticated client stations to ensure they are active. If no response is received and the number of retries is reached, the client station is disconnected.

Parameters

<interval>	Specify how long to wait between polls.
<retries>	Specify how many polls a client station can fail to reply to before it is disconnected.

Description

This feature enables the controller to detect if two client stations are using the same IP address but have different MAC addresses. If this occurs, access is terminated for this IP address removing both stations from the network.

Changing these values may have security implications. A large interval provides a greater opportunity for a session to be hijacked.

The initial query is always done after the client station has been idle for 60 seconds. If there is no answer to this query, the settings for Interval and Retries are used to control additional retries.

system accounting

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
system accounting
```

Enables RADIUS accounting support.

```
no system accounting
```

Disables RADIUS accounting support.

remember delay

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
remember delay <number>
```

Length of time to remember users. Users who return later than this delay interval, are presented with the login page instead of being re-authenticated.

remember html users

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`remember html users`

Enables support for remembering (automatically re-authenticating) HTML-authenticated users who leave the network but return within the remember delay interval.

`no remember html users`

Disables support for remembering HTML-authenticated users.

worldpay installation id

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`worldpay installation id <string>`

Sets the installation ID for the WorldPay payment service.

worldpay payment response password

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`worldpay payment response password <string>`

Sets the payment response password for the WorldPay payment service.

worldpay payment url

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`worldpay payment url <string>`

Sets the payment URL for the WorldPay payment service.

authorize_net installation id

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`authorize_net installation id <string>`

Sets the login ID for the Authorize.Net payment service.

authorize_net payment url

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`authorize_net payment url <string>`

Sets the payment URL for the Authorize.Net payment service.

authorize_net transaction key

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`authorize_net transaction key <string>`

Sets the transaction key for the Authorize.Net payment service.

show paypal

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show paypal`

Shows LLDP statistics for all ports or a specific port .

paypal api-url

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`paypal api-url (default | url) [<url>]`

Set or unset a custom PayPal API URL.

paypal operation-mode

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`paypal operation-mode (test | production)`

Set the PayPal operation mode (test or production)

paypal password

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`paypal password <string>`

Set the password for the PayPal payment service.

paypal signature

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`paypal signature <string>`

Set the signature for the PayPal payment service.

paypal user-id

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`paypal user-id <string>`

Set the User ID for the PayPal payment service.

ads presentation with frameset

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ads presentation with frameset`

Enables ad presentation to redirect to the frameset-ads-page instead of the ads-page.

`no ads presentation with frameset`

Disables the frameset for ad presentation, causing ad presentation to only use the ads-page.

authentication http

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`authentication http <number>`

Sets the port number the controller will be used to provide standard HTTP access to the management tool.

HTTP connections made to this port are met with a warning and the browser is redirected to the secure web server port. By default this parameter is set to port 80.

authentication https

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`authentication https <number>`

Sets the port number the controller will use to provide secure access to the management tool (HTTPS). By default this parameter is set to port 443.

local welcome-page

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`local welcome-page`

Enables the presentation of the local welcome-page on successful authentication.

`no local welcome-page`

Disables the presentation of the local welcome-page on successful authentication.

noc access internet

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`noc access internet`

Accept authentication requests on the Internet port.

`no noc access internet`

Do not accept authentication requests on the Internet port.

noc access vpn

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`noc access vpn`

Accept authentication requests on VPN connections.

`no noc access vpn`

Do not accept authentication requests on VPN connections.

noc allow

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`noc allow <ip address>/<mask>`

Adds an IP address or subnet to the list of destinations that the controller will accept user login authentication requests from when NOC authentication is active.

`no noc allow <ip address>/<mask>`

Removes the specified IP address or subnet from the list of destinations that the controller will accept user login authentication requests from when NOC authentication is active.

When the list is empty, authentication requests are accepted from any address.

noc authentication

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`noc authentication`

Enables support for NOC authentication.

`no noc authentication`

Disables support for NOC authentication.

secure login

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`secure login`

Enables secure login.

`no secure login`

Disables secure login.

sslv2 authentication

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`sslv2 authentication`

Enables sslv2 authentication.

`no sslv2 authentication`

Disables sslv2 authentication.

user-agent block

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`user-agent block <agent>`

Adds a user agent that the controller will not redirect HTTP login requests coming from this agent when user-agent filtering is active.

`no user-agent block <agent>`

Removes the specified user agent from the list of agents that the controller will not redirect HTTP login requests coming from this list agents when user-agent filtering is active.

When the list is empty, HTTP login requests are redirected for all client applications.

user-agent filtering

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`user-agent filtering`

Enables user agent filtering.

`no user-agent filtering`

Disables user agent filtering.

noc access interface vlan

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`noc access interface vlan <name>`

Adds the specified VLAN to the list of interfaces that authentication requests are accepted on.

`no noc access interface vlan <name>`

Removes the specified VLAN from the list of interfaces that authentication requests are accepted on.

noc access interface gre

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`noc access interface gre <name>`

Adds the specified GRE tunnel to the list of interfaces that authentication requests are accepted on.

`no noc access interface gre <name>`

Removes the specified GRE tunnel from the list of interfaces that authentication requests are accepted on.

ipass id

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ipass id <name>`

Specifies the WISPr location ID assigned to the controller.

`no ipass id`

Deletes the WISPr location ID assigned to the controller.

ipass name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ipass name <name>`

Specifies the WISPr location name assigned to the controller.

`no ipass name`

Deletes the WISPr location name assigned to the controller.

wispr abort login url

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`wispr abort login url <url>`

Specifies the WISPr abort login url assigned to the controller.

`no wispr abort login url`

Deletes the WISPr abort login url assigned to the controller.

wispr login url

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`wispr login url <url>`

Specifies the WISPr login url assigned to the controller.

`no wispr login url`

Deletes the WISPr login url assigned to the controller.

wispr logoff url

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`wispr logoff url <url>`

Specifies the WISPr logoff url assigned to the controller.

`no wispr logoff url`

Deletes the WISPr logoff url assigned to the controller.

access-list

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`access-list <index> <rule>`

Adds a new rule to an access list at the specified index position.

`no use access-list`

Do not use an access list.

Parameters

`index`	Index position of the rule within the access list.
`rule`	Access list rule definition in the format: *<listname>*[,OPTIONAL],*<action>*,*<protocol>*,*<address>*,*<port>*[,*<account>*[,*<interval>*]]
<listname>	Specifies a name (up to 32 characters long) to identify the access list this rule applies to. If a list with this name does not exist, a new list is created. If a list with this name exists, the rule is added to it.
`OPTIONAL`	Allows the access list to be activated even if this rule fails to initialize. For example, if you specify a rule that contains an address which cannot be resolved for some reason, the other rules that make up the access list will still be initialized. If you do not specify optional, a failed rule will cause the entire list to fail. Critical access list definitions (such as for a remote login page, certificates) should not use the OPTIONAL setting because if these definitions fail to initialize there will be no indication in the log.
<action>	Specifies what action the rule takes when it matches incoming traffic. Two options are available:

- ACCEPT - Allow traffic matching this rule.
- DENY - Reject traffic matching this rule.
- WARN - Redirect traffic matching this rule to an error page.

<protocol>	Specify the protocol to check: tcp, udp, icmp, all
<address>	Specify one of the following:

- IP address or domain name (up to 107 characters in length)
- Subnet address. Include the network mask as follows: address/subnet mask For example: 192.168.30.0/24
- Use the keyword **all** to match any address.
- Use the keyword **none** if the protocol does not take an address range (ICMP for example).

<port> Specify a specific port to check or a port range as follows:

- none: Used with ICMP (since it has no ports).
- all: Check all ports.
- 1-65535[:1-65535] - Specify a specific port or port range.

<account> Specify the name of the user account the controller will send billing information to for this rule. Account names must be unique and can be up to 32 characters in length.

<interval> Specify time between interim accounting updates. If you do not enable this option, accounting information is only sent when a user connection is terminated. Range: 5-99999 seconds in 15 second increments.

use access-list

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`use access-list <listname>`

Specifies the name of the access list to use.

`no use access-list`

Do not use an access list.

use access-list unauth

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`use access-list unauth <listname>`

Specifies the name of the access list to use for unauthenticated stations (list disappears once authenticated).

`no use access-list unauth`

Do not use an access list for unauthenticated stations (list disappears once authenticated).

config file

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`config file <url>`

Specifies the URL that points to a new configuration file to load.

`no config file`

Do not load a new configuration file.

http proxy upstream

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`http proxy upstream <string>`

Specifies the host:port of the HTTP Proxy Upstream server.

`no http proxy upstream`

Do not use an HTTP Proxy Upstream server.

https ssl certificate

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`https ssl certificate <url>`

Specifies the URL that points to an SSL certificate that will replace the default certificate on the controller.

`no https ssl certificate`

Do not load a custom SSL certificate.

mac-address

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`mac-address <macaddr> [<username>] [<password>]`

Adds a MAC address to the local configuration list.

When the MAC authentication option is enabled (in a VAP (VSC) profile), you can define local configuration settings to validate MAC addresses.

Parameters

`macaddr`	MAC address of the device as 12 hexadecimal numbers, with the values 'a' to 'f' in lowercase. For example: 0003520a0f01.
`username`	Username assigned to the device.
`password`	Password assigned to the device.

fail page

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`fail page <url>`

Specifies the URL of a new fail page.

`no fail page`

No new fail page. Use default.

goodbye url

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`goodbye url <url>`

Specifies the URL of a goodbye page.

`no goodbye url`

No goodbye page.

ipass login url

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ipass login url <url>`

Specifies the URL of the IPass login page. The controller will automatically redirect users with IPass client software to this page.

`no ipass login url`

No IPass login URL

login error url

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`login error url <url>`

Specifies the URL of a login error page.

`no login error url`

No login error page.

login page

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`login page <url>`

Specifies the URL of the new login page.

`no login page`

No new login page. Use default.

login url

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`login url <url>`

Specifies the URL of a remote login page.

`no login url`

No remote login page.

logo

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`logo <url>`

Specifies the URL of a new logo.

`no logo`

No new logo. Use default.

messages

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`messages <url>`

Specifies the URL of a new message file.

`no messages`

No new messages file. Use default.

noc ssl ca-certificate

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`noc ssl ca-certificate <url>`

Specifies the URL of the certificate from the certificate authority (CA) that issued the NOC certificate.

`no noc ssl ca-certificate`

No CA certificate.

noc ssl certificate

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`noc ssl certificate <url>`

Specifies the URL of the certificate issued to the application on the remote web server that will send user info to the controller for authentication.

`no noc ssl certificate`

No certificate.

session page

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`session page <url>`

Specifies the URL of a new session page.

`no session page`

No new session page. Use default.

transport page

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`transport page <url>`

Specifies the URL of a new transport page.

`no transport page`

No new transport page. Use default.

welcome url

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`welcome url <url>`

Specifies the URL of a welcome page.

`no welcome url`

No welcome page.

notify user location changes

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`notify user location changes`

Notify RADIUS on location changes.

`no notify user location changes`

Do not notify RADIUS on location changes.

Default user session profile context

Path: View > Enable > Config > Default user session profile

Use this context to define default settings for user sessions. Most of these attributes can be overridden by adding settings to a user's RADIUS account.

In this context, all commands add an attribute to the list, in some cases (access-list & mac-address) several entries are added. The "no" form will remove the attributes.

accounting interim update

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`accounting interim update <number>`

Sets the default accounting interim update interval (in seconds) for all users that do not have a specific interval set in their profile.

`no accounting interim update`

Removes this attribute.

idle timeout

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`idle timeout <number>`

Sets the default idle time out for all users that do not have a specific limit set in their profile.

`no idle timeout`

Removes this attribute.

maximum input octets

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`maximum input octets <value>`

Sets the maximum input limit in octets for all users that do not have a specific limit set in their profile.

`no maximum input octets`

Removes this attribute.

maximum input packets

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`maximum input packets <number>`

Sets the maximum input limit in packets for all users that do not have a specific limit set in their profile.

`no maximum input packets`

Removes this attribute.

maximum output octets

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`maximum output octets <value>`

Sets the maximum output limit in octets for all users that do not have a specific limit set in their profile.

`no maximum output octets`

Removes this attribute.

maximum output packets

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`maximum output packets <number>`

Sets the maximum output limit in packets for all users that do not have a specific limit set in their profile.

`no maximum output packets`

Removes this attribute.

maximum total octets

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`maximum total octets <value>`

Sets the maximum total limit in octets for all users that do not have a specific limit set in their profile.

`no maximum total octets`

Removes this attribute.

maximum total packets

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`maximum total packets <number>`

Sets the maximum total limit in packets for all users that do not have a specific limit set in their profile.

`no maximum total packets`

Removes this attribute.

nat one-to-one

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`nat one-to-one`

Enables one-to-one NAT support for all users that do not have a specific value set in their profile.

`no nat one-to-one`

Removes this attribute.

session timeout

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`session timeout <number>`

Sets the default session timeout for all users that do not have a specific limit set in their profile.

`no session timeout`

Removes this attribute.

smtp redirection setup

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`<hostname>[:<port>t][,<username>,<password>]`

Sets basic SMTP redirection info: hostname[:port][,username,password].

`no smtp redirection setup`

Clears basic SMTP redirection info.

Parameters

<hostname>	Specify the IP address or domain name of the e-mail server. Maximum length is 253 characters.
<port>	Specify the port on the e-mail server to relay to. Range: 1 to 65535. Default: 25
<username>	Specify the username required to log on to the SMTP server. Maximum 32 characters.
<password>	Specify the password required to log on to the SMTP server. Maximum 32 characters.

Description

Sets the default SMTP server address for all user sessions. This attribute is used if a specific server is not set for a particular user

public ip subnet

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`public ip subnet`

Enables the use of the public IP subnet for IP Addressing for all users that do not have a specific value set in their profile.

`no public ip subnet`

Removes this attribute.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`end`

Switches to parent context.

smtp redirection

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`smtp redirection`

Enables SMTP proxy support.

`no smtp redirection`

Disables SMTP proxy support.

Session profile context

Path: View > Enable > Config > Session profile

Use this context to define settings for a user's session profile.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
end
```

Switches to parent context.

access controlled

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
access controlled
```

Set profile as access-controlled.

```
no access controlled
```

Set profile as non-access-controlled.

access list

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
access list <name>
```

Sets the access list.

```
use access list
```

Use this access list.

```
no use access list
```

Do not use this access list.

accounting interim update

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
accounting interim update <number>
```

Sets the default accounting interim update interval (in seconds) for all users that do not have a specific interval set in their profile.

```
use accounting interim update
```

Use attribute.

```
no use accounting interim update
```

Removes this attribute.

arp polling interval

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`arp polling interval <number>`

Sets the ARP polling interval.

`use arp polling interval`

Use the ARP polling interval.

`no use arp polling interval`

Do not use the ARP polling interval.

arp polling max count

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`arp polling max count <number>`

Sets the polling ARP count.

`use arp polling max count`

Use the polling ARP count.

`no use arp polling max count`

Do not use the polling ARP count.

bandwidth level

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`bandwidth level (very-high | high | normal | low)`

Sets Bandwidth level.

`use bandwidth level`

Use Bandwidth level.

`no use bandwidth level`

Don't use Bandwidth level.

egress vlan

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`egress vlan <number>`

Sets the tunnel private group id.

`use egress vlan`

Use the tunnel private group id.

`no use egress vlan`

Do not use the tunnel private group id.

idle timeout

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`idle timeout <number>`

Sets the default idle time out for all users that do not have a specific limit set in their profile.

`use idle timeout`

Use this attribute.

`no use idle timeout`

Removes this attribute.

intercept traffic

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`intercept traffic`

Turn on legal traffic interception.

`no intercept traffic`

Turn off legal traffic interception.

`use intercept traffic`

Use legal traffic interception.

`no use intercept traffic`

Do not use legal traffic interception.

max input rate

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`max input rate <number>`

Sets the maximum input rate.

`use max input rate`

Use the maximum input rate.

`no use max input rate`

Do not use the maximum input rate.

max output rate

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`max output rate <number>`

Sets the maximum output rate.

`use max output rate`

Use the maximum output rate.

`no use max output rate`

Do not use the maximum output rate.

nat one-to-one

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`nat one-to-one`

Enables one-to-one NAT support for all users that do not have a specific value set in their profile.

`no nat one-to-one`

Removes this attribute.

`use nat one-to-one`

Use this attribute.

`no use nat one-to-one`

Do not use this attribute.

session profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`session profile <name>`

Change this profile's name.

smtp redirection setup

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`smtp redirection setup <hostname>[:<port>t][,<username>,<password>]`

Sets basic SMTP redirection info: hostname[:port][,username,password].

`no smtp redirection setup`

Clears basic SMTP redirection info.

`use smtp redirection setup`

Use SMTP redirection.

`no use smtp redirection setup`

Do not use SMTP redirection.

Parameters

<hostname>	Specify the IP address or domain name of the e-mail server. Maximum length is 253 characters.
<port>	Specify the port on the e-mail server to relay to. Range: 1 to 65535. Default: 25
<username>	Specify the username required to log on to the SMTP server. Maximum 32 characters.
<password>	Specify the password required to log on to the SMTP server. Maximum 32 characters.

Description

Sets the default SMTP server address for all users sessions. This attribute is used if a specific server is not set for a particular user

termination action

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`termination action (logout | reauthenticate)`

Sets the termination action.

`use termination action`

Use the termination action.

`no use termination action`

Do not use the termination action.

user defined attribute

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`user defined attribute <name>:<type>:<vendor-id>:<vendor-type>:<format>:<value>`

Add a new user defined attribute.

`no user defined attribute <description>`

Add a new user-defined attribute.

Parameters

<name>	Friendly name for this attribute.
<type>	Numerical RADIUS type, 26 is Vendor-Specific.
<vendor-id>	If RADIUS type is 26, contains the Vendor-Id. Put 0 if not.
<vendor-type>	If RADIUS type is 26, contains the Vendor-Type. Put 0 if not.
<format>	Is one of: 'integer', 'address', 'text', 'string' or 'time'.
<value>	Contains the actual value.

Format description and values:

- integer: value is a numerical string.
- address: value is a legal IP address, or possibly a host name.
- text: value is any string of alphanumerical characters.
- string: value is a series of hexadecimal digits.
- time: value is a time string.

For related information, see RFC 2138, Section 5.

public ip subnet

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`public ip subnet`

Set profile to use the public IP subnet for IP Addressing once authenticated.

`no public ip subnet`

Removes this attribute.

`use public ip subnet`

Use this attribute.

```
no use public ip subnet
```

Do not use this attribute.

User account context

Path: View > Enable > Config > User account

Use this context to modify settings for a specific user account in the local user list.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
end
```

Switches to parent context.

access controlled

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
access controlled
```

Makes this user access controlled.

```
no access controlled
```

Makes this user not access controlled.

access-controlled profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
access-controlled profile <name>
```

Use this session profile for this account.

```
no access-controlled profile <name>
```

Do not use this session profile for this account.

```
use access-controlled profile
```

Use the Access Controlled profiles.

```
no use access-controlled profile
```

Use the Access Controlled profiles.

access-controlled virtual ap

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
access-controlled virtual ap <name>
```

Adds to the list of allowed virtual APs.

```
no access-controlled virtual ap <name>
```

Removes from the list of allowed virtual APs.

```
use access-controlled virtual ap
```

Use only allowed Virtual AP (VSC) for this profile.

```
no use access-controlled virtual ap
```

Use any Virtual AP (VSC) for this profile.

active

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`active`

Enables this user account.

`no active`

Disables this user account.

chargeable user identity

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`chargeable user identity <id>`

Sets the CUI.

`use chargeable user identity`

Uses the CUI.

`no use chargeable user identity`

Do not use the CUI.

control method

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`control method (subscription | endtime | none)`

egress vlan

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`egress vlan <number>`

Sets the VLAN tunnel ID.

`use egress vlan`

Use the VLAN tunnel ID.

`no use egress vlan`

Do not use the VLAN tunnel ID.

end time

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`end time <time>`

Sets expiration time: \"YYYY-MM-DD HH:MM:SS\".

idle timeout

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`idle timeout <number>`

Sets the idle timeout for this user.

`no idle timeout`

This user never times out.

max user sessions

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`max user sessions <number>`

Sets the maximum concurrent sessions for this user.

`no max user sessions`

This user doesn't have a maximum concurrent sessions limit.

password

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`password <secret>`

Change the password for this user.

regular profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`regular profile <name>`

Apply a non-access-controlled profile.

`no regular profile <name>`

Remove a non-access-controlled profile.

`use regular profile`

Use the non-access-controlled profiles.

`no use regular profile`

Do not use the non-access-controlled profiles.

regular virtual ap

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`regular virtual ap <name>`

Add to the list of allowed virtual APs.

`no regular virtual ap <name>`

Remove from the list of allowed virtual APs.

`use regular virtual ap`

Use only allowed Virtual AP (VSC) for this profile.

session timeout

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`session timeout <number>`

Sets the session timeout for this user.

```
no session timeout
```

This user session never times out.

subscription plan

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
subscription plan <name>
```

Sets the subscription plan to use.

```
no subscription plan
```

Delete a subscription plan.

username

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
username <name>
```

Change the name for this user.

Internet port interface context

Path: View > Enable > Config > Internet port interface

Use this context to configure the Internet port.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
end
```

Switches to parent context.

duplex

Supported on: MSM710 E-MSM720 MSM760

```
duplex (auto | half | full)
```

Sets the duplex mode on Internet.

Parameters

`auto`	Lets the controller automatically set duplex mode based on the type of equipment it is connected to.
`half`	Forces the port to operate in half duplex mode.
`full`	Forces the port to operate in full duplex mode.

speed

Supported on: MSM710 E-MSM720 MSM760

```
speed (auto | 10 | 100)
```

Sets the speed of the Internet port.

Parameters

`auto`	Lets the controller automatically set port speed based on the type of equipment it is connected to.
`100`	Forces the port to operate at 100 mbps.
`10`	Forces the port to operate at 10 mbps.

interface vlan

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
interface vlan <networkname>
```

Switches to the specified VLAN interface or create a new VLAN interface with the specified VLAN definition.

```
no interface vlan <networkname>
```

Deletes the specified VLAN.

ipsec vlan interface

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ipsec vlan interface <name>`

Specifies which VLAN is used by IPsec.

`no ipsec vlan interface`

Do not use a VLAN for IPsec.

LAN port interface context

Path: View > Enable > Config > LAN port interface

Use this context to configure the LAN port.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
end
```

Switches to parent context.

duplex

Supported on: MSM710 E-MSM720 MSM760

```
duplex (auto | half | full)
```

Sets the duplex mode on LAN.

Parameters

`auto`	Lets the controller automatically set duplex mode based on the type of equipment it is connected to.
`half`	Forces the port to operate in half duplex mode.
`full`	Forces the port to operate in full duplex mode.

speed

Supported on: MSM710 E-MSM720 MSM760

```
speed (auto | 10 | 100)
```

Sets the speed of the LAN port.

Parameters

`auto`	Lets the controller automatically set port speed based on the type of equipment it is connected to.
`100`	Forces the port to operate at 100 mbps.
`10`	Forces the port to operate at 10 mbps.

interface vlan

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
interface vlan <id>[-<id2>]
```

Switches to the specified VLAN interface or create a new VLAN interface with the specified ID.

```
no interface vlan <id>[-<id2>]
```

Deletes the specified VLAN interface.

Parameters

<id>	VLAN ID. Range: 1 - 4094.
<id2>	VLAN ID. When specified, is the last value in a range.

ipsec vlan interface

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ipsec vlan interface <name>`

Specifies which VLAN is used by IPsec.

`no ipsec vlan interface`

Do not use a VLAN for IPsec.

WAN IP interface context

Path: View > Enable > Config > WAN IP interface

Use this context to configure various IP-networking related settings on the Internet port.

pppoe client user

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`pppoe client user <username> <password>`

Sets the PPPoE username and password.

`no pppoe client user`

Deletes the PPPoE username.

Parameters

<username>	The username assigned to you by your ISP. The controller will use this username to log on to your ISP when establishing a PPPoE connection.
<password>	The password assigned to you by your ISP. The controller will use this username to log on to your ISP when establishing a PPPoE connection.

New

tagged

Supported on: E-MSM720

`tagged <port>`

Tags the current VLAN on the specified port.

`no tagged <port>`

Removes the current VLAN from the specified port.

New

untagged

Supported on: E-MSM720

`untagged <port>`

Untags the current VLAN on the specified port.

`no untagged <port>`

Removes the current VLAN from the specified port.

ip address mode

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ip address mode (dhcp | pppoe | static | none)`

Sets the IP addressing mode for Internet.

Parameters

dhcp	Dynamic host configuration protocol. The DHCP server will automatically assign an address to the controller, which functions as a DHCP client.
pppoe	Point-to-point protocol over Ethernet. The PPPoE server will automatically assign an IP address to the controller. You need to supply a username and password so the controller can log on.

`static`	This option enables you to manually assign an IP address to the controller.
`none`	No IP address.

ip address

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ip address <ip address>/<mask>`

Sets a static IP address for the port.

Parameters

`<address>`	IP address.
`</mask>`	Subnet mask in CIDR format. Specifies the number of bits in the mask.

ip nat

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ip nat`

Enables Network Address Translation.

`no ip nat`

Disables Network Address Translation.

nat limit port range

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`nat limit port range`

Reserves a range of TCP and UDP ports for each user starting at port 5000.

`no nat limit port range`

Use any port for NAT.

All outgoing traffic for the user is mapped within the range. Applications that set an incoming port (Active FTP, for example) may choose a port that is outside of the allocated port range. If you enable this feature you should not assign static NAT mappings in the range 5000 to 32768.

nat limit port range size

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`nat limit port range size <number>`

Determine the size of the range to use per user, this will limit the number of user authentication supported if too high.

ip address dhcp client-id

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ip address dhcp client-id <id>`

Specifies an ID to identify the controller to a DHCP server. This parameter is not required by all ISPs.

`no ip address dhcp client-id`

Deletes the specified DHCP client id.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`end`

Switches to parent context.

pppoe auto-reconnect

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`pppoe auto-reconnect`

The controller will automatically attempt to reconnect if the connection is lost.

`no pppoe auto-reconnect`

The controller will not automatically attempt to reconnect if the connection is lost.

pppoe mru

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`pppoe mru <bytes>`

Specifies the maximum receive unit.

Changes to this parameter should only be made according to the recommendations of your ISP. Incorrectly setting this parameter can reduce the throughput of your Internet connection.

Parameters

<bytes>	Maximum size (in bytes) of a PPPoE packet when receiving. Range: 500 - 1500 bytes.

pppoe mtu

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`pppoe mtu <bytes>`

Specifies the maximum transmit unit.

Changes to this parameter should only be made according to the recommendations of your ISP. Incorrectly setting this parameter can reduce the throughput of your Internet connection.

Parameters

<bytes>	Maximum size (in bytes) of a PPPoE packet when transmitting. Range: 500 - 1500 bytes.

pppoe unnumbered

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`pppoe unnumbered`

Enable unnumbered mode.

`no pppoe unnumbered`

Disable unnumbered mode.

This feature is useful when the controller is connected to the Internet and NAT is not being used. Instead of assigning two IP addresses to the controller, one to the Internet port and one to the LAN port, both ports can share a single IP address. This is especially useful when a limited number of IP addresses are available to you.

ip nat outside source static

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ip nat outside source static (tcp|udp) <visible-port> <internal-addr> <internal-port>`

Adds a static NAT mapping which routes the specified incoming traffic to the specified IP address on the internal network.

Parameters

`tcp | udp`	Selects the protocol that the mapping will operate on.
<visible-port>	The protocol port number that the incoming traffic uses.
<internal addr>	IP address of the device on the internal network that traffic will be routed to.
<internal-port>	The protocol port number that the incoming traffic will be mapped to.

ip address alternate

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ip address alternate <ip address> [<ip address>]`

Assigns an alternate IP addresses to the Internet port. The address must be valid on the Internet.

`no ip address alternate <ip address> [<ip address>]`

Deletes the specified alternate IP address.

The controller uses these addresses to support its one-to-one NAT feature. The controller will not respond to pings directed at these IP addresses:

LAN IP interface context

Path: View > Enable > Config > LAN IP interface
View > Enable > Config > LAN IP interface

Use this context to configure various IP-networking related settings on the LAN port.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`end`

Switches to parent context.

ip address

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ip address <ip address>/<mask>`

Sets a static IP address for the port.

Parameters

<address>	IP address.
</mask>	Subnet mask in CIDR format. Specifies the number of bits in the mask.

ip address management

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ip address management <ip address>/<mask>`

Sets a management IP address for this device.

Parameters

<address>	IP address.
</mask>	Subnet mask in CIDR format. Specifies the number of bits in the mask.

New

tagged

Supported on: E-MSM720

`tagged <port>`

Tags the current VLAN on the specified port.

`no tagged <port>`

Removes the current VLAN from the specified port.

New

untagged

Supported on: E-MSM720

`untagged <port>`

Untags the current VLAN on the specified port.

`no untagged <port>`

Removes the current VLAN from the specified port.

Public access RADIUS attributes context

Path: View > Enable > Config > Public access RADIUS attributes

Use this context to setup retrieval of public access attributes from a RADIUS server.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`end`

Switches to parent context.

active

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`active`

Use a RADIUS server to fetch configuration information for the public access network.

`no active`

Do not use a RADIUS server for remote configuration.

credentials

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`credentials <username> <password>`

Sets the username/password to use for RADIUS configuration.

`no credentials`

Resets the username/password to use for RADIUS configuration.

interval

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`interval <number>`

Sets the intervals at which the controller will retrieve configuration information from the RADIUS server.

radius server profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius server profile <name>`

Sets the RADIUS profile to use.

`no radius server profile`

Do not use a RADIUS profile.

Virtual AP context

Path: View > Enable > Config > Virtual AP

Use this context to configure VSC profiles (formerly called VAPs).

By default, one VSC profile exists with the name "HP". This is the default profile and cannot be deleted.

virtual ap name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`virtual ap name <name>`

Change the VAP (VSC) name.

access control

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`access control`

Sets this profile to use the services of the controller's access control mechanism for authentication and control of client sessions.

`no access control`

Do not provide access control with this VAC (VAP).

When enabled

- The controller provides a variety of methods for user authentication, including: MAC, 802.1X, and HTML via either the local user list or a RADIUS server.
- Egress traffic can be routed based on the user state: authenticated, unauthenticated, or intercepted.

When disabled

- The controller does not perform user authentication, either via RADIUS or the local user list. All authentication must be handled by a remote device.
- All wireless traffic is bridged to an egress VLAN.
- No access controller functions are available. This means no support for RADIUS attributes for the controller.
- 802.1X support is available, including support for RADIUS attributes for users.

force centralize data

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`force centralize data`

Force use of the client data tunnel even when the AP is L2 connected to the controller.

`no force centralize data`

Automatically determine if the client data tunnel is required.

ingress interface

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ingress vlan <name>`

Sets the specified interface as the ingress interface traffic will be accepted on.

This command takes a *selector* as its input. A selector is used to differentiate traffic, and decide which parameters should be used to select the VAP (VSC) this user/traffic applies to.

egress unauthenticated

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`egress ( unauthenticated | authenticated | intercepted ) ( default | vlan <vlan-name> | gre <gre-name>)`

Sets the output interface that this profile forwards data traffic to.

Parameters

`unauthenticated`	This is any traffic from client stations that have not attempted to be authenticated by the controller. For example, a client station that fails to authenticate via 802.1X is not considered to be unauthenticated.
`authenticated`	This is any traffic from client stations that have been authenticated by the controller and given access to the public access interface.
`intercepted`	Traffic from specific users can be intercepted and redirected. To enable traffic interception for a specific user, you must specify the appropriate setting in their RADIUS account. See the controller Administrator's Guide for details.
`default`	Sends traffic without specifying a specific interface. The interface that is used will be selected by the routing module based on the traffic destination
<vlan-name>	Sends traffic tagged with the VLAN ID defined for the specified VLAN name.
<gre-name>	Sends traffic on the specified GRE tunnel.

guest-mode

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`guest-mode`

Enables broadcast of the wireless network name (SSID).

`no guest-mode`

Disables broadcast of the wireless network name (SSID).

max-association

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`max-association <stations>`

Sets the maximum number of clients stations that can associate with this VAP (VSC).

<stations>	Number of client stations. Range: 1 - 255.

ssid name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ssid name <name>`

Specifies the WLAN name (SSID) for the profile.

encryption key 1

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`encryption key <key> <value>`

Sets WEP key 1.

`no encryption key <key>`

Deletes WEP key 1.

Parameters

<key>	WEP key number. Range: 1 - 4. Keys 2 to 4 are only supported on the first WLAN profile.
<value>	Key value. The number of characters you specify for a key determines the level of encryption the controller will provide. For 40-bit encryption, specify 5 ASCII characters or 10 HEX digits. For 128-bit encryption, specify 13 ASCII characters or 26 HEX digits.

encryption key format

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`encryption key format (hex | ascii)`

Specify the WEP key format.

Parameters

`hex`	Hex keys should only include the following digits: 0-9, a-f, A-F
`ascii`	ASCII keys are much weaker than carefully chosen hex keys. You can include ASCII characters between 32 and 126, inclusive, in the key. However, note that not all client stations support non-alphanumeric characters such as spaces, punctuation, or special symbols in the key.

transmit key

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`transmit key <key number>`

Sets the key the controller will use to encrypt transmitted data. All four keys are used to decrypt received data.

Parameters

<key number>	Transmit key number. Range: 1 -4.

authentication server access controller

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
authentication server access controller
```

Use the access controller to authenticate 802.1X or WPA logins.

authentication server accounting

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
authentication server accounting
```

Enables RADIUS accounting for this VSC (VAP).

```
no authentication server accounting
```

Disables RADIUS accounting for this VSC (VAP).

authentication server accounting radius profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
authentication server accounting radius profile <name>
```

Sets RADIUS accounting to use the specified RADIUS profile.

```
no authentication server accounting radius profile
```

Removes accounting support for 802.1X.

authentication server radius

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
authentication server radius <name>
```

Sets the RADIUS profile to use for 802.1X or WPA authentication.

dot1x authentication

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
dot1x authentication (local | radius | active-directory)
```

Sets the authentication for 802.1X and WPA.

wpa-psk

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
wpa-psk <key>
```

Sets the WPA preshared key.

```
no wpa-psk
```

Deletes the WPA preshared key.

Parameters

`password`	Specify a key that is between 8 and 64 ASCII characters in length. It is recommended that the preshared key be at least 20 characters long, and be a mix of letters and numbers.

Description

The controller uses the key you specify to generate the TKIP keys that encrypt the wireless data stream. Since this is a static key, it is not as secure as using dynamically generated keys.

authentication server request radius cui

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
authentication server request radius cui
```

Include in the authentication request a request for a CUI.

dot1x session page

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
dot1x session page
```

802.1X authenticated users will be presented with the Session page and the Welcome page after a successful authentication.

```
no dot1x session page
```

802.1X authenticated users will NOT be presented with the Session page and the Welcome page after a successful authentication.

New

wpa terminate controller

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
wpa terminate controller
```

Enable terminate WPA at the controller

```
no wpa terminate controller
```

Disable terminate WPA at the controller

wireless filters

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
wireless filters
```

Enables the wireless security filters which only allow traffic to flow between the controller and a specific upstream device (such as a HP service controller).

```
no wireless filters
```

Do not limit traffic flow between the controller and an upstream device.

This prevents wireless users from accessing resources on the backbone LAN that interconnects the controller and the upstream device.

wireless filters mac

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
wireless filters mac <mac>
```

Sets the MAC address of the upstream device to send traffic to.

```
no wireless filters mac <mac>
```

Deletes the MAC address of the upstream device to send traffic to.

wireless filters rule input

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`wireless filters rule input <rule>`

Adds a custom filter definition for incoming wireless traffic.

Use this command to define custom security filters for incoming wireless traffic. Filters are specified using standard pcap syntax (http://www.tcpdump.org/tcpdump_man.html) with the addition of a few HP-specific placeholders. These placeholders can be used to refer to specific MAC addresses and are expanded by the controller when the filter is activated. Once expanded, the filter must respect the pcap syntax. The pcap syntax is documented in the tcpdump man page:

Placeholders

- %a - MAC address of the access controller.
- %b - MAC address of the bridge.
- %g - Mac address of the default gateway assigned to the controller.
- %w - MAC address of wireless port.

wireless filters rule output

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`wireless filters rule output <rule>`

Adds a custom filter definition for outgoing wireless traffic.

Use this command to define custom security filters for outgoing wireless traffic. Filters are specified using standard pcap syntax (http://www.tcpdump.org/tcpdump_man.html) with the addition of a few HP-specific placeholders. These placeholders can be used to refer to specific MAC addresses and are expanded by the controller when the filter is activated. Once expanded, the filter must respect the pcap syntax. The pcap syntax is documented in the tcpdump man page:

Placeholders

- %a - MAC address of the access controller.
- %b - MAC address of the bridge.
- %g - Mac address of the default gateway assigned to the controller.
- %w - MAC address of wireless port.

wireless filters type

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`wireless filters type (mac | gateway | rules)`

Sets the type of wireless security filter to use.

Parameters

`mac`	Traffic is forwarded to an upstream device with a specific MAC address. Wireless security filters use the default definitions.
`gateway`	Traffic is forwarded to the default gateway assigned to the controller. Wireless security filters use the default definitions.
`custom`	Lets you define custom security filters and address for the upstream device.

Description

The controller features an intelligent bridge which can apply security filters to safeguard the flow of wireless traffic. The filters limit both incoming and outgoing traffic as defined below, and force the controller to exchange traffic with a specific upstream device. If the controller is configured to use the services of a HP access controller, then the default security filters are automatically enabled and all traffic is sent to the access controller.

Default filters for incoming wireless traffic

Applies to traffic sent from wireless client stations to the controller.

Accepted

- Any IP traffic addressed to the access controller.
- PPPoE traffic (The PPPoe server must be the upstream device.)
- IP broadcast packets, except NetBIOS
- Certain address management protocols (ARP, DHCP) regardless of their source address.
- Any traffic addressed to the controller, including 802.1X.

Blocked

- All other traffic is blocked. This includes NetBIOS traffic regardless of its source/destination address. TTPS traffic not addressed to the controller (or upstream device) is also blocked, which means wireless client stations cannot access the management tool on other HP products.

Default filters for outgoing wireless traffic

Applies to traffic sent from the controller to wireless client stations.

Accepted

- Any IP traffic coming from the upstream device, except NetBIOS packets.
- PPPoE traffic from the upstream device.
- IP broadcast packets, except NetBIOS
- ARP and DHCP Offer and ACK packets.
- Any traffic coming from the controller itself, including 802.1X.

Blocked

- All other traffic is blocked. This includes NetBIOS traffic regardless of its source/destination address.

mac-filters local

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
mac-filters local
```

Enables the MAC filter list.

```
no mac-filters local
```

Disables the MAC filter list.

mac-filters

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`mac-filters <address>`

Adds an address to the MAC filter list.

`no mac-filters <address>`

Remove the specified address from the MAC filter list.

Parameters

<address>	MAC address. Specify 6 pairs of hexadecimal numbers separated by colons, with the values a to f in lowercase. For example: 00:00:00:0a:0f:01

Description

This feature enables you to control access to the controller based on the MAC address of client stations. You can either block access or allow access, depending on your requirements. When both this option and the MAC-based authentication options are enabled, the following applies: if a user's MAC address does not appear in the MAC filtering list, then MAC-based authentication takes place for that user.

mac-filters mode

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`mac-filters mode (allow | block)`

Either allow or block access to the wireless network for client stations whose addresses appear in the MAC filter list.

mac authentication accounting

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`mac authentication accounting`

Enables RADIUS accounting for this VAP (VSC).

`no mac authentication accounting`

Disables RADIUS accounting for this VAP (VSC).

mac authentication accounting radius profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`mac authentication accounting radius profile <name>`

Sets RADIUS accounting to use the specified RADIUS profile.

`no mac authentication accounting radius profile`

Disables accounting support for MAC authentication.

mac authentication radius profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`mac authentication radius profile <radiusname>`

Specifies the name of the RADIUS profile to use for MAC-based authentication.

`no mac authentication radius profile`

Do not use a RADIUS profile.

mac authentication remote

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`mac authentication remote`

Sets MAC-based authentication to use a RADIUS profile.

`no mac authentication remote`

MAC-based authentication will not use a RADIUS profile.

mac authentication request radius cui

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`mac authentication request radius cui`

Include a request for a CUI in authentication requests.

mac authentication local

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`mac authentication local`

Sets MAC-based authentication to use the local user list to validate the MAC addresses of client stations.

`no mac authentication local`

Do not use the local user list for MAC-based authentication.

mac authentication

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`mac authentication`

Enables support for MAC-based authentication.

`no mac authentication`

Disable support for MAC-based authentication.

html authentication

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`html authentication`

Enables HTML authentication.

`no html authentication`

Disables HTML authentication.

html authentication accounting

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`html authentication accounting`

Enables RADIUS accounting.

`no html authentication accounting`

Disables RADIUS accounting.

html authentication accounting radius profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`html authentication accounting radius profile <name>`

Sets RADIUS accounting for HTML users to use the specified RADIUS profile.

`no html authentication accounting radius profile`

Disables RADIUS accounting RADIUS support for HTML users.

html authentication active-directory

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`html authentication active-directory`

Use Active Directory (AD) to authenticate users.

`no html authentication active-directory`

Do not use Active Directory (AD) to authenticate users.

html authentication local

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`html authentication local`

Validate HTML logins using the local user list.

`no html authentication local`

Do not validate HTML logins using the local user list.

html authentication radius

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`html authentication radius`

Validate HTML logins using the specified RADIUS profile.

`no html authentication radius`

Do not validate HTML logins using the specified RADIUS profile.

html authentication radius profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`html authentication radius profile <name>`

Validate HTML logins using the specified RADIUS profile.

`no html authentication radius profile`

Do not validate HTML logins using the specified RADIUS profile.

html authentication request radius cui

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`html authentication request radius cui`

Include a request for a CUI in the authentication request.

`no html authentication request radius cui`

Do not include a request for a CUI in the authentication request.

html authentication timeout

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`html authentication timeout <number>`

Sets the HTML authentication timeout.

active

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`active`

Enable this VAP (VSC).

`no active`

Disable this VAP (VSC).

band steering

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`band steering`

Enable band steering on this VSC between both radios.

`no band steering`

Disable band steering on this VSC between both radios.

beacon dtim count

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`beacon dtim count <number>`

Defines the DTIM period in the beacon.

Client stations use the DTIM to wake up from low-power mode to receive multicast traffic. The controller transmits a beacon every 100 ms. The DTIM counts down with each beacon that is sent, therefore if the DTIM is set to 5, then client stations in low-power mode will wake up every 500 ms (.5 second) to receive multicast traffic.

beacon transmit power

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
beacon transmit power
```

Advertise the current transmit power setting in the beacon.

```
no beacon transmit power
```

Do not advertise the current transmit power setting in the beacon.

broadcast filter

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
broadcast filter
```

Improve performance by not sending most broadcasts.

```
no broadcast filter
```

Send all broadcasts over wireless.

data rate

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
data rate (a | b | g | bg | n) <rate>
```

Enable the given data rate for a particular PHY type.

```
no data rate (a | b | g | bg | n) <rate>
```

Disable the given data rate for a particular PHY type.

public forwarding

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
public forwarding (any | 802.1x | none | ipv6)
```

Enables support for traffic exchange between wireless client stations.

access lan stations

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
access lan stations
```

Permits traffic exchange between wireless and wired users.

```
no access lan stations
```

Blocks traffic exchange between wireless and wired users.

fast authentication

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
fast authentication
```

Enables WPA2 opportunistic key caching.

```
no fast authentication
```

Disables WPA2 opportunistic key caching.

layer3 mobility

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
layer3 mobility
```

Enables Layer 3 mobility.

```
no layer3 mobility
```

Disables Layer 3 mobility.

layer3 mobility hns fallback method

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
layer3 mobility hns (subnet | vlan | home)
```

Select the home network selection (HNS) fallback method. Used when VLAN-based method is selected and no VLAN RADIUS attribute is used.

Parameters

`subnet`	Determine the home network based on subnet.
`vlan`	Determine the home network using the configured home VLAN.
`home`	Assume the user at its home network.

layer3 mobility hns method

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
layer3 mobility hns (subnet | vlan)
```

Select the home network selection (HNS) method.

Parameters

`subnet`	Determine the home network based on subnet.
`vlan`	Determine the home network using the received VLAN RADIUS attribute.

add ip-qos profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
add ip-qos profile <name>
```

Adds the specified profile to the list of IP QoS profiles in effect for this VSC (VAP).

<profile-name>	Name of an existing IP QoS profile.

delete ip-qos profile all

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
delete ip-qos profile all
```

Clears the list of IP QoS profiles currently in effect for this VSC (VAP).

delete ip-qos profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
delete ip-qos profile <name>
```

Removes the specified profile from the list of IP QoS profiles in effect for this VSC (VAP).

<profile-name>	Name of an existing IP QoS profile currently in the profile list for this VSC (VAP).

qos

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
qos ( 802.1p | very-high | high | normal | low | diffsrv | tos | default | vap0
| vap1 | vap2 | vap3)
```

Sets the QoS level for this profile.

```
no qos
```

Disables QoS for this profile.

Four traffic queues are provided based on the WME standard. In order of priority, these queues are:

- 1: Voice traffic
- 2: Video traffic
- 3: Best effort data traffic
- 4: Background data traffic

Each QoS priority mechanism maps traffic to one of the four traffic queues. Client stations that do not support the QoS mechanism for the profile they are connected to are always assigned to queue 3.

Important: Traffic delivery is based on strict priority (per the WME standard). Therefore, if excessive traffic is present on queues 1 or 2, it will reduce the flow of traffic on queues 3 and 4.

`802.1p`	Traffic from 802.1p client stations is classified based on the VLAN priority field present within the VLAN header. When this mechanism is selected, the controller will advertise WME capabilities, enabling WME clients to associate and take advantage of them. This setting has no effect on legacy clients. Note: To support 802.1p, the wireless profile must have a VLAN assigned to it, which means that client station traffic is forwarded onto the LAN port only.
`vap0 to vap3`	Allows a specific priority level to be specified for all traffic on a VAP (VSC) profile. This enables client stations without a QoS mechanism to set traffic priority by connecting to the appropriate SSID. If you enable this priority mechanism, it takes precedence regardless of the priority mechanism supported by associated client stations. For example, if you set SSID-based low priority for a profile, all devices that connect to the profile have their traffic set at this priority Mapping to the traffic queues is as follows: vap0 or very-high=queue 1, vap1 or high=queue 2, vap2 or normal=queue 3, vap3 or low=queue 4
`diffsrv`	Differential services is a method for defining IP traffic priority on a per-hop basis. The Differential Service bits are defined in RFC2474 and are composed of the six most significant bits of the IP TOS field. These bits define the class selector code points which the CN320 maps to the appropriate traffic queue. (default setting)
`tos`	The IP TOS (type of service) field can be used to mark prioritization or special handling for IP packets.

upstream diffserv tagging

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
upstream diffserv tagging
```

Enables upstream diffserv tagging.

```
no upstream diffserv tagging
```

Disables upstream diffserv tagging.

wmm advertising

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
wmm advertising
```

Enables WMM information element advertising.

```
no wmm advertising
```

Disables WMM information element advertising.

html redirection

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
html redirection
```

Enables support for HTML logins.

```
no html redirection
```

Disables support for HTML logins.

local nas id

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
local nas id <nasid>
```

Set the NAS Id when only local authentication is configured.

```
use local nas id
```

Enables the use of NAS Id when only local authentication is configured.

```
no use local nas id
```

Disables the use of NAS Id when only local authentication is configured.

bandwidth

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
bandwidth (very-high | high | normal | low)
```

Sets the bandwidth level.

bandwidth default rates

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
bandwidth default rates
```

Enables default bandwidth rates for this VAP (VSC).

`no bandwidth default rates`

Disables default bandwidth rates for this VAP (VSC).

bandwidth default rates maximum

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`bandwidth default rates maximum <max-tx-rate> <max-rx-rate>`

Sets the default maximum transmit and receive rates.

radius accounting realms

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius accounting realms`

Use RADIUS accounting realms.

`no radius accounting realms`

Do not use RADIUS accounting realms.

radius authentication realms

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius authentication realms`

Use RADIUS authentication realms.

`no radius authentication realms`

Do not use RADIUS authentication realms.

identify stations by ip only

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`identify stations by ip only`

Identify stations based on IP address only.

`no identify stations by ip only`

Do not identify stations based on address IP only.

location-aware group

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`location-aware group <name>`

Sets the specified group name for the access point.

`no location-aware group`

Deletes the specified group name for the access point.

location-aware called-station-id content

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`location-aware called-station-id content (ssid | group | mac)`

Sets the value returned in Called-Station-ID.

dhcp relay

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dhcp relay <primary-ip-address> <[secondary-ip-address]>`

Sets the primary and secondary DHCP server for the relay.

`no dhcp relay`

Resets the primary and secondary DHCP server for the relay.

dhcp relay active

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dhcp relay active`

The dhcp relay is enabled on the VAP (VSC).

`no dhcp relay active`

The dhcp relay is not enabled on the VAP (VSC).

dhcp relay circuit id

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dhcp relay circuit id <string>`

Sets the Option 82 circuit ID.

`no dhcp relay circuit id`

Clears the Option 82 circuit ID.

dhcp relay remote id

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dhcp relay remote id <string>`

Sets the Option 82 remote ID.

`no dhcp relay remote id`

Clears the Option 82 remote ID.

dhcp relay subnet

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dhcp relay subnet <ip address>/<mask>`

Sets the DHCP relay subnet.

`no dhcp relay subnet`

Clears the DHCP relay subnet.

dhcp server

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dhcp server`

The dhcp server is enabled on the VAP (VSC).

`no dhcp server`

The dhcp server is not enabled on the VAP (VSC).

dhcp server dns

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dhcp server dns <ip address>`

Sets the domain name server provided to DHCP clients.

`no dhcp server dns`

Reset the domain name server provided to DHCP clients.

dhcp server gateway

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dhcp server gateway <ip address>`

Sets the default gateway provided to DHCP clients.

`no dhcp server gateway`

Reset the default gateway provided to DHCP clients.

dhcp server range

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dhcp server range <start-range> <end-range>`

Specify the DHCP server IP address range.

dhcp server subnet

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dhcp server subnet <ip address>/<mask>`

Sets the DHCP server subnet.

`no dhcp server subnet`

Clears the DHCP server subnet.

radius-framed-protocol-attribute

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius-framed-protocol-attribute`

Include the RADIUS Framed-Protocol attribute in Access Request packets. The value for this attribute is PPP (1).

```
no radius-framed-protocol-attribute
```

Do not include the RADIUS Framed-Protocol attribute in Access Request packets.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
end
```

Switches to parent context.

security

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
security (none | wep | 802.1X [wep | static-wep] | wpa (psk | radius) [ v1 | v2 ] )
```

Sets the current wireless security policy.

Parameters

`none`	No wireless security.
`wep`	This option enables support for wireless users with WEP client software.
`802.1X`	This option enables support for wireless users with 802.1X client software. The controller supports 802.1X client software that uses EAP-TLS, EAP-TTLS, EAP-SIM, and PEAP.
`wep`	Enables the use of dynamic WEP keys for all 802.1X sessions. Dynamic key rotation occurs on key 1, which is the broadcast key. Key 0 is the pairwise key. It is automatically generated by the controller.
`static-wep`	Support client stations using static WEP keys.
`wpa`	This option enables support for wireless users with WPA client software.
`psk`	Enables support for a preshared key.
`radius`	The controller obtains the MPPE key from the RADIUS server. This is a dynamic key that changes each time the user logs in and is authenticated. The MPPE key is used to generate the TKIP keys that encrypt the wireless data stream.
`v1,v2`	Specify which version of WPA to use. None will use both versions (mixed mode).

Interface context

Path: View > Enable > Config > Interface

Use this context to configure an physical interface (port).

New

duplex-mode

Supported on: E-MSM720

`duplex-mode (auto | half | full)`

Sets the duplex mode for the current port.

New

end

Supported on: E-MSM720

`end`

Switches to parent context.

New

flow-control

Supported on: E-MSM720

`flow-control`

Enables flow control on the current port.

`no flow-control`

Disables flow control on the current port.

New

flow-control auto-negotiation

Supported on: E-MSM720

`flow-control auto-negotiation`

Enables flow control auto negotiation on the current port.

`no flow-control auto-negotiation`

Disables flow control auto negotiation on the current port.

New

speed

Supported on: E-MSM720

`speed (auto | 10 | 100 | 1000 | 10-100)`

Sets the speed for the current port.

New

trunk group

Supported on: E-MSM720

`trunk group <group>`

Sets the trunk group number when "trunk type" is set to "trunk".

New

trunk type

Supported on: E-MSM720

```
trunk type (none | lacp | trunk)
```

Sets the trunk type for the current port.

VLAN interface context

Path: View > Enable > Config > VLAN interface
View > Enable > Config > Internet port interface > VLAN interface
View > Enable > Config > LAN port interface > VLAN interface

Use this context to configure VLANs.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`end`

Switches to parent context.

ip address

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ip address <ip address>/<mask>`

Sets a static IP address for the VLAN.

Parameters

<address>	IP address.
</mask>	Subnet mask in CIDR format. Specifies the number of bits in the mask.

ip address mode

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ip address mode (dhcp | static | none)`

Sets the IP addressing mode for this VLAN interface.

Parameters

`dhcp`	Dynamic host configuration protocol. The DHCP server will automatically assign an address to the controller, which functions as a DHCP client.
`static`	This option enables you to manually assign an IP address to the controller.
`none`	This VLAN does not have an IP address.

New

tagged

Supported on: E-MSM720

`tagged <port>`

Assigns the current VLAN to the specified port as tagged.

`no tagged <port>`

Removes the current VLAN from the specified port.

New

untagged

Supported on: E-MSM720

`untagged <port>`

Assigns the current VLAN to the specified port as untagged.

`no untagged <port>`

Removes the current VLAN from the specified port.

ip default-gateway

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ip default-gateway <ip address>`

Sets the default gateway for this VLAN.

`no ip default-gateway`

Removes the default gateway for this VLAN.

ip nat

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ip nat`

Enables Network Address translation for this interface.

`no ip nat`

Disables Network Address translation for this interface.

RADIUS profiles context

Path: View > Enable > Config > RADIUS profiles

Use this context to define RADIUS profiles. These profiles are used to establish a connection with RADIUS servers.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`end`

Switches to parent context.

radius-server accounting port

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius-server accounting port <number>`

Specifies the port to use for RADIUS accounting.

Parameters

<number>	Accounting port number. Range: 1 - 65535.

radius-server alternate hosts

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius-server alternate hosts`

Try last answering RADIUS host first.

`no radius-server alternate hosts`

Try primary RADIUS host first.

radius-server authentication method

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius-server authentication method (mschap | chap | mschapv2 | pap | eap-md5)`

Sets the authentication method to use when communicating with the RADIUS server.

For 802.1X users, the authentication method is always determined by the 802.1X client software and is not controlled by this setting.

If traffic between the controller and the RADIUS server is not protected by a VPN, it is recommended that you use either EAP-MD5 or MSCHAP V2, if supported by your RADIUS Server. (PAP, MSCHAP V1 and CHAP are less secure protocols.)

radius-server authentication port

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius-server authentication port <number>`

Specifies the port to use for RADIUS authentication. By default, RADIUS servers use port 1812.

Parameters

<number>	Authentication port number. Range: 1 - 65535

radius-server deadtime

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius-server deadtime <seconds>`

Sets the retry interval for access and accounting requests that time-out.

If no reply is received within this interval, the controller switches between the primary and secondary RADIUS servers (if defined). If a reply is received after the interval expires, it is ignored.

Parameters

<seconds>	Retry interval. Range: 2 - 60 seconds.

radius-server host

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius-server host <primary>[<secondary>]`

Sets the addresses of the primary and secondary RADIUS servers.

Parameters

<primary>	IP address of the primary RADIUS server.
<secondary>	IP address of the secondary RADIUS server.

radius-server key 2

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius-server key <primary>[<secondary>]`

Sets the primary and secondary secrets used to connect with the RADIUS server.

Parameters

<primary>	Shared secret for the primary RADIUS server.
<secondary>	Shared secret for the secondary RADIUS server.

radius-server message-authenticator

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius-server message-authenticator`

Include the message authenticator attribute in RADIUS packets.

`no radius-server message-authenticator`

Do not include the message authenticator attribute in RADIUS packets.

radius-server name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius-server name <name>`

Changes the name of the RADIUS profile.

radius-server nasid

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius-server nasid <id>`

Sets the network access server ID you want to use for the controller.

By default, the serial number of the controller is used. The controller includes the NAS-ID attribute in all packets that it sends to the RADIUS server.

radius-server timeout

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius-server timeout`

Activates RADIUS timeout.

`no radius-server timeout`

Disables RADIUS timeout.

radius-server timeout

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius-server timeout <number>`

Sets the total timeout for RADIUS requests.

`no radius-server timeout`

Disables RADIUS timeout.

radius-server force-nas-port-to-vlanid

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius-server force-nas-port-to-vlanid`

Force the NAS-Port attribute to ingress VLAN ID in RADIUS packets.

`no radius-server force-nas-port-to-vlanid`

Do not force the NAS-Port attribute to ingress VLAN ID in RADIUS packets.

radius-server realm

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius-server realm (regex | text)`

Specifies if realms in list are regular expressions or just plain text.

radius-server realm name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radius-server realm name <name>`

Adds the specified realm name.

`no radius-server realm name <name>`

Removes the specified realm name.

IP QOS context

Path: View > Enable > Config > IP QOS

Use this context to configure IP QoS profiles.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`end`

Returns to a previous context.

end-port

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`end-port <number>`

Specifies the end port to use for this IP QoS profile.

Parameters

<number>	End port number. Range: 0 - 65535

priority

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`priority <low | medium | high | very-high>`

Sets the priority for this IP QoS profile.

Parameters

<priority>	Available priorities are: low, medium, high and very-high.

profile name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`profile name <name>`

Changes the name of the IP QoS profile.

protocol

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`protocol <number>`

Specifies the protocol ID to use for this IP QoS profile.

Parameters

<number>	Protocol number. Range: 0 - 255.

start-port

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`start-port <number>`

Specifies the start port to use for this IP QoS profile.

Parameters

<number>	Start port number. Range: 0 - 65535

DHCP server context

Path: View > Enable > Config > DHCP server

Use this context to configure DHCP server settings.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`end`

Switches to parent context.

active

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`active`

This range is enabled.

`no active`

This range is not enabled.

gateway

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`gateway <ip address>`

Sets the default gateway provided to DHCP clients.

`no gateway`

Reset the default gateway provided to DHCP clients.

range

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`range <start-range> <end-range>`

Specify the DHCP server IP address range.

permanent leases

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`permanent leases <ip address> <macaddr> <uid>`

Adds a permanent DHCP lease for this mapping.

`no permanent leases <ip address> <macaddr> <uid>`

Deletes a permanent DHCP lease for this mapping.

GRE interface context

Path: View > Enable > Config > GRE interface

Use this context to configure GRE tunnels.

end force

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`end [force]`

Quits the GRE context.

gre name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`gre name <name>`

Renames the current GRE interface.

ip address

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ip address <ip address>/<mask>`

Set the local tunnel IP address and mask.

peer ip address

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`peer ip address <ip address>`

Sets the GRE peer IP address.

remote ip address

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`remote ip address <ip address>`

Sets the remote tunnel IP address.

IPsec context

Path: View > Enable > Config > IPsec

Use this context to define IPSec configuration settings.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`end`

Switches to parent context.

active

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`active`

Enables policy.

`no active`

Disables policy.

authentication

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`authentication (x509 | psk)`

Selects between x509 and psk authentication.

cipher

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`cipher aes`

Sets the desired encryption algorithm.

`no cipher aes`

Do not use this encryption algorithm.

dns domain

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dns domain <names>`

Sets the domain name for this policy.

`no dns domain <names>`

Resets the domain name for this policy.

dns server

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dns server ( <ip address> | none )`

Sets the DNS server for this policy.

`no dns server`

Resets the DNS server for this policy.

incoming nat

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`incoming nat`

Enables NAT for incoming traffic.

`no incoming nat`

Disables NAT for incoming traffic.

incoming traffic network

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`incoming traffic network <ip address>/<mask>`

Sets the Phase 2 incoming network.

interface

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`interface (lan | internet)`

Sets the interface this policy applies to.

local id

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`local id (ip-address <ip address> | host <name> | email <address> | dn <dn>)`

Specify the local id type and value.

mode

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`mode (main | aggressive) (tunnel | transport)`

Sets the IPSec mode.

outgoing traffic network

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`outgoing traffic network <ip address>/<mask>`

Sets the Phase 2 outgoing network.

peer id

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`peer id (ip-address <ip address> | host <name> | email <address> | dn <dn>)`

Sets the peer id type and value.

peer ip address

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
peer ip address (<ip address>| any )
```

Sets the peer ip address for this policy.

perfect forward secrecy

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
perfect forward secrecy
```

Enables PFS.

```
no perfect forward secrecy
```

Disables PFS.

preshared key

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
preshared key <secret>
```

Sets the preshared key.

```
no preshared key
```

Removes the preshared key.

Syslog context

Path: View > Enable > Config > Syslog

Use this context to define syslog settings.

active

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
active
```

Enables logging to the current destination.

```
no active
```

Disables logging to the current destination.

logging facility

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
logging facility (local0 | local1 | local2 | local3 | local4 | local5 | local6 |
local7)
```

Sets the facility that is used when logging messages to a syslog server.

Parameters

<facility> Available facilities are: local0 - local7.

logging host

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
logging host (tcp | udp) <addr> [<number>]
```

Sets the remote address, the connection protocol and port of current syslog remote destination.

logging prefix

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
logging prefix <string>
```

Sets the prefix that will be prepended to all syslog messages.

```
no logging prefix
```

Removes the prefix that is prepended to all syslog messages.

name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
name <name>
```

Renames the current syslog destination.

logging source

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
logging source (local | controlled_aps | controllers | all)
```

Sets the source used when logging messages to a syslog server.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
end
```

Switches to parent context.

level

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
level
```

Enables filtering of the log file by severity level.

```
no level
```

Disables filtering of the log file by severity level.

level

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
level (lower | higher) (debug | info | notice | warning | error | critical |
alert | emergency)
```

Defines the severity of messages that will be logged.

```
no level
```

Disables filtering of the log file by severity level.

Parameters

`debug`	Debug-level messages.
`info`	Informational messages.
`notice`	Normal, but significant condition.
`warning`	Warning conditions.
`error`	Error conditions.
`critical`	Critical conditions.
`alert`	Action must be taken immediately.
`emergency`	System is unusable.

matches

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
matches (any | all) filters
```

All three log file filters (message, process, and level) are combined to filter the log according to this setting.

message

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`message`

Enables filtering of the log file message field.

`no message`

Disables filtering of the log file message field.

message

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`message (matches | notmatches) <regex>`

Use this filter to include log messages. Use a regular expression to define the match criteria for the log file message field.

`no message`

Disables filtering of the log file message field.

process

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`process`

Enables filtering of the log file by process name.

`no process`

Disables filtering of the log file by process name.

process

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`process (matches | notmatches) <string>`

Use this filter to include log messages according to their process name.

`no process`

Disables filtering of the log file by process name.

PPTP client interface

Path: View > Enable > Config > PPTP client interface

Use this context to configure the PPTP client.

active

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`active`

Sets PPTP client connection to 'up'.

`no active`

Sets PPTP client connection to 'down'.

pptp client credentials

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`pptp client credentials <name> <password>`

Sets the PPTP username and password.

pptp client domain name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`pptp client domain name <name>`

Sets the domain name used by the PPTP client.

pptp client server address

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`pptp client server address <address>`

Sets the IP address to connect to.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`end`

Switches to parent context.

ip nat

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ip nat`

Enables NAT for the PPTP client.

`no ip nat`

Disables NAT for the PPTP client.

pptp client auto route discovery

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
pptp client auto route discovery
```

Enables auto-route discovery.

```
no pptp client auto route discovery
```

Disables auto-route discovery.

pptp client lcp echo

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
pptp client lcp echo
```

Enables PPTP LCP echo.

```
no pptp client lcp echo
```

Disables PPTP LCP echo.

Keychain context

Path: View > Enable > Config > Keychain

Use this context to manage a keychain.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`end`

End current context.

key

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`key <number>`

Enter new key.

`no key <number>`

Deletes key with given ID.

key chain name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`key chain name <name>`

Renames current keychain.

Keys context

Path: View > Enable > Config > Keychain > Keys

Use this context to configure the keys that are part of a keychain.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
end
```

End current context.

key-string

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
key-string <name>
```

Set the authentication string for this key.

```
no key-string
```

Remove the authentication string for this key.

Subscription plan context

Path: View > Enable > Config > Subscription plan

Use this context to define settings for subscription plans.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`end`

End current context.

daily restriction

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`daily restriction <from> <to>`

Sets the daily restrictions hours.

`use daily restriction`

Enable daily restrictions.

`no use daily restriction`

Disable daily restrictions.

end time

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`end time <datetime>`

Set the account end date and time. \"YYYY-MM-DD HH:MM:SS\".

`use end time`

Use account end time.

`no use end time`

Do not use account end time.

initial login time allocation

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`initial login time allocation <number> (minutes | hours | days)`

Sets the amount of time allocated after the first login by a user.

`use initial login time allocation`

Use the initial login time allocation.

`no use initial login time allocation`

Do not use the initial login time allocation.

online time limit

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`online time limit`

Use the online time limit.

`no online time limit`

Do not use the online time limit.

online time limit

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`online time limit <number> (minutes | hours | days)`

Sets the initial online time for an account.

`no online time limit`

Do not use the online time limit.

start time

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`start time <datetime>`

Set the account start date and time. \"YYYY-MM-DD HH:MM:SS\".

`use start time`

Use account start time.

`no use start time`

Do not use account start time.

subscription plan name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`subscription plan name <newname>`

Changes the subscription plan name.

public ip reservation

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`public ip reservation`

Enables public IP address reservation.

`no public ip reservation`

Disables public IP address reservation.

public ip subnet

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`public ip subnet`

Set profile to use the public IP subnet for IP Addressing once authenticated.

`no public ip subnet`

Removes this attribute.

`use public ip subnet`

Use this attribute.

`no use public ip subnet`

Do not use this attribute.

SNMP user context

Path: View > Enable > Config > SNMP user

Use this context to define settings for SNMP users.

access level

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
access level (read-only | read-write)
```

Specifies the access level use for this SNMP user.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
end
```

Returns to a previous context.

password

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
password <password>
```

Specifies the password use for this SNMP user.

security

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
security (md5-des | sha-aes)
```

Specifies the security use for this SNMP user.

user name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
user name <name>
```

Changes the name of the SNMP user.

SNMP notification receiver context

Path: View > Enable > Config > SNMP notification receiver

Use this context to configure SNMP notification receivers.

community

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`community <community>`

Specifies the community for this SNMP notification receiver.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`end`

Returns to a previous context.

port

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`port <number>`

Specifies the UDP port use for this SNMP notification receiver.

receiver

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`receiver <host>`

Changes the host name of the SNMP notification receiver.

user

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`user <name>`

Specifies the username for this SNMP notification receiver.

version

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`version (1 | 2c | 3)`

Specifies the SNMP version for this SNMP notification receiver.

Active Directory Group context

Path: View > Enable > Config > Active Directory Group

Use this context to define the attributes to send when a user is related to an Active Directory group.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
end
```

Switches to parent context.

access controlled

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
access controlled
```

Make this user access-controlled.

```
no access controlled
```

Make this user non-access-controlled.

access-controlled profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
access-controlled profile <name>
```

Use this session profile for this account.

```
no access-controlled profile <name>
```

Do not use this session profile for this account.

```
use access-controlled profile
```

Use the Access Controlled profiles.

```
no use access-controlled profile
```

Do not use the Access Controlled profiles.

access-controlled virtual ap

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
access-controlled virtual ap <name>
```

Add to the list of allowed virtual APs (VSCs).

```
no access-controlled virtual ap <name>
```

Remove from the list of allowed virtual APs (VSCs).

```
use access-controlled virtual ap
```

Use only allowed Virtual APs (VSCs) for this profile.

```
no use access-controlled virtual ap
```

Use any Virtual APs (VSCs) for this profile.

active

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`active`

Enable this user account.

`no active`

Disable this user account.

active-directory group name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`active-directory group name <name>`

Change the name for this user.

egress vlan

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`egress vlan <number>`

Set the VLAN tunnel ID.

`use egress vlan`

Use the VLAN tunnel ID.

`no use egress vlan`

Do not use the VLAN tunnel ID.

regular profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`regular profile <name>`

Apply a non-access-controlled profile.

`no regular profile <name>`

Remove a non-access-controlled profile.

`use regular profile`

Use the non-access controlled profiles.

`no use regular profile`

Do not use the non-access controlled profiles.

regular virtual ap

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`regular virtual ap <name>`

Add to the list of allowed virtual APs (VSCs).

`no regular virtual ap <name>`

Remove from the list of allowed virtual APs (VSCs).

`use regular virtual ap`

Use only allowed Virtual APs (VSCs) for this profile.

`no use regular virtual ap`

Use any Virtual AP (VSC) for this profile.

Controlled APs context

Path: View > Enable > Controlled APs

Use these commands to configure controlled APs.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`end`

Switches to parent context.

execute action

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`execute action (synchronize | accept-suspicious | accept-product | rediscover)`

Execute an action on the entity's devices.

execute system action

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`execute system action (restart | reset | switch-mode)`

Execute a system action on the AP.

show config factory

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show config [factory]`

Displays the current configuration as a list of CLI commands.

ap group

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ap group <name>`

Change the AP group (must Synchronize).

ap name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ap name <name>`

Change the current AP name.

config

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`config`

Switch to generic configuration context.

contact

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
contact <name>
```

Modify the contact.

location

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
location <name>
```

Modify the location.

product type

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
product type (map-320 | map-330 | map-625 | map-630 | msm410 | e-msm430 | e-msm460 | e-msm466 | msm317 | msm318 | e-msm466-r)
```

Modify the default product type.

product type

Supported on: MSM710

```
product type (wi2-sr-1)
```

Modify the default product type.

Controlled APs group context

Path: View > Enable > Controlled APs group

Use this context to configure controlled AP groups.

execute action

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`execute action (synchronize | accept-suspicious | accept-product | rediscover)`

Execute an action on the entity's devices.

show config factory

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show config [factory]`

Displays the current configuration as a list of CLI commands.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`end`

Switch to parent context.

config

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`config`

Switch to generic configuration context.

group name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`group name <name>`

Change the current group name.

virtual ap binding

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`virtual ap binding <vapprofile>`

Create/use a VAP (VSC) binding.

`no virtual ap binding <vapprofile>`

Delete a VAP (VSC) binding.

Controlled APs base group context

Path: View > Enable > Controlled APs base group

Use this context to configure the base controlled APs group.

execute action

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
execute action (synchronize | accept-suspicious | accept-product | rediscover)
```

Execute an action on the entity's devices.

show config factory

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
show config [factory]
```

Displays the current configuration as a list of CLI commands.

config

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
config
```

Switch to generic configuration context.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
end
```

Switch to parent context.

Controlled APs network configuration context

Path: View > Enable > Controlled APs > Controlled APs network configuration
View > Enable > Controlled APs group > Controlled APs network configuration
View > Enable > Controlled APs base group > Controlled APs network configuration

Use this context to define network settings for controlled APs.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
end
```

interface wireless

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
interface wireless <number> [<product>]
```

Switch to the wireless interface context.

local mesh group

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
local mesh group <group>
```

Switch to local mesh group context.

local mesh provisioning group

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
local mesh provisioning group
```

Switch to the local mesh provisioning group context.

provisioning connectivity

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
provisioning connectivity
```

Switch to the provisioning connectivity context.

provisioning discovery

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
provisioning discovery
```

Switch to the provisioning discovery context.

radius profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
radius profile <profile>
```

Switch to controlled network radius profile context.

show tech

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show tech`

Displays technical information.

switch port

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`switch port <name>`

Switch to the ethernet port context.

syslog

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`syslog`

Switch to the syslog context.

inherit vlan port2

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`inherit vlan port2`

Inherit settings from parent.

`no inherit vlan port2`

Do not inherit settings from parent.

vlan port2

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`vlan port2`

Enable VLAN on port 2.

`no vlan port2`

Disable VLAN on port 2.

vlan port2 id

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`vlan port2 id <vlanid>`

Sets the vlan ID.

inherit country code

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`inherit country code`

Inherit settings from parent.

`no inherit country code`

Do not inherit settings from parent.

world-mode dot11 country code

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`world-mode dot11 country code <code>`

Specifies the country in which the controller is operating.

Parameters

<code>	An ISO3166 three-letter country code.

New

inherit ipv6 ra conversion

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`inherit ipv6 ra conversion`

Inherit IPv6 RA conversion settings from parent.

`no inherit ipv6 ra conversion`

Do not inherit IPv6 RA conversion settings from parent.

New

ipv6 ra conversion

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ipv6 ra conversion`

Enables IPv6 Router Advertisement (RA) multicast conversion which ensures that the controller properly assigns IP addresses to IPv6 clients according to their VLAN.

`no ipv6 ra conversion`

Disables IPv6 Router Advertisement (RA) multicast conversion.

New

show ipv6 ra conversion

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`show ipv6 ra conversion`

Displays the IPv6 RA conversion state.

sensor server name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`sensor server name <name>`

Sets the IP address or hostname of the RF Manager Server to connect to.

Parameters

`Name`	Specify the IP address of the RF Manager Server or its hostname. If a hostname is specified, the controller must be able to resolve it via DNS,Âîthat is, an entry must be created on the network DNS server that points to the IP address of the RF Manager Server.

sensor server id

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`sensor server id <id>`

Sets the server ID of the RF Manager Server to connect to.

Parameters

`ID`	Specify the Server ID of the RF Manager Server to connect to. Set the Server ID to 0 to have the controller send a discovery request to all active HP RF Manager Servers. The controller will connect to the first server that responds to the discovery request.

sensor discovery mode

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`sensor discovery mode (id | ip)`

Sets the method the controller will use to communicate with the RF Manager Server.

Parameters

`id`	Connect using the Server ID of the RF Manager Server.
`ip`	Connect using the IP address or hostname of the RF Manager Server.

Description

For these methods to work, the following must be true:

- The controller must be able to reach the RF Manager Server via a network connected to port 1 or port 2. For example, you should be able to ping the RF Manager Server's IP address from the controller.
- If there are any firewalls between the controller and the RF Manager Server, then TCP and UDP ports 3851 must be open bi-directionally.
- If using the hostname option, an entry must be created on the network DNS server that points to the IP address of the RF Manager Server.
- If using the Server ID option, support for multicast traffic must be enabled on all routers and switches connected between the controller and the RF Manager Server.

sensor network detector

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`sensor network detector`

Enable the Network Detector.

`no sensor network detector`

Disable the Network Detector.

inherit sensor

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`inherit sensor`

Inherit sensor settings from parent.

```
no inherit sensor
```

Do not inherit sensor settings from parent.

dynamic key

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
dynamic key
```

Enables dynamic key support for 802.1X and WPA.

```
no dynamic key
```

Disables dynamic key support for 802.1X and WPA.

dynamic key interval

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
dynamic key interval (5m | 10m | 15m | 30m | 1h | 2h | 4h | 8h | 12h)
```

Specifies how often (in minutes or hours) that the group (broadcast) key is changed for 802.1X and WPA.

dot1x reauth

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
dot1x reauth
```

Enable this option to force 802.1X client stations to reauthenticate.

```
no dot1x reauth
```

Disables 802.1X reauthentication.

dot1x reauth period

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
dot1x reauth period (15m | 30m | 1h | 2h | 4h | 8h | 12h)
```

Sets the 802.1X reauthentication interval. Client stations must reauthenticate when this interval expires.

dot1x reauth terminate

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
dot1x reauth terminate
```

Enable this option to allow client stations to remain connected during re-authentication. Client traffic is blocked only when re-authentication fails.

```
no dot1x reauth terminate
```

Disabled this option to block client traffic during re-authentication and only activate traffic again if authentication succeeds.

dot1x supplicant timeout

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dot1x supplicant timeout <number>`

Sets the 802.1X supplicant time-out.

Parameters

<seconds> time-out in seconds.

inherit 8021x

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`inherit 802.1x`

Inherit 802.1X settings from parent.

`no inherit 802.1x`

Do not inherit 802.1X settings from parent.

bridge protocol ieee

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`bridge protocol ieee`

Enable the bridge spanning tree protocol to prevent undesirable loops from occurring in the network that may result in decreased throughput.

`no bridge protocol ieee`

Disable the bridge spanning tree protocol.

inherit untagged stp

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`inherit untagged stp`

Inherit untagged spanning tree protocol settings from parent.

`no inherit untagged stp`

Do not inherit untagged spanning tree protocol settings from parent.

bridge protocol ieee vlan

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`bridge protocol ieee vlan`

Enable the bridge spanning tree protocol for VLANs.

`no bridge protocol ieee vlan`

Disable the bridge spanning tree protocol for VLANs.

inherit vlan stp

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
inherit vlan stp
```

Inherit vlan spanning tree protocol settings from parent.

```
no inherit vlan stp
```

Do not inherit vlan spanning tree protocol settings from parent.

inherit local mesh qos

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
inherit local mesh qos
```

Inherit local mesh QoS settings from parent.

```
no inherit local mesh qos
```

Do not inherit local mesh QoS settings from parent.

local mesh ip qos profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
local mesh ip qos profile <profile>
```

Add an IP Qos profile to the profile's list.

```
no local mesh ip qos profile <profile>
```

Delete an IP QoS profile from the profile's list.

local mesh qos mechanism

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
local mesh qos mechanism (disabled | 802.1p | very_high | high | normal | low |
diffsrv | tos | ip_qos)
```

Set the QoS priority mechanism.

enable vsc services

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
enable vsc services
```

Enable wireless services when the controller is unreachable.

```
no enable vsc services
```

Shut down wireless services when the controller is unreachable.

inherit service availability

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
inherit service availability
```

Inherit service availability from parent.

`no inherit service availability`

Do not inherit service availability from parent.

inherit l3subnets

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`inherit l3subnets`

Inherit subnets from parent.

`no inherit l3subnets`

Do not inherit L3 subnets from parent.

l3subnet

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`l3subnet <vlanid> <ipsubnet> <ipnetmask>`

Add a new subnet to the list.

`no l3subnet <vlanid> <ipsubnet> <ipnetmask>`

Delete an l3subnet from the list.

inherit switch port _

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`inherit switch port <port_number>`

Inherit settings from the switch ports.

`no inherit switch port <port_number>`

Inherit settings from the switch ports.

inherit switch ports

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`inherit switch ports`

Inherit settings from the switch ports.

`no inherit switch ports`

Inherit settings from the switch ports.

inherit lldp-app-profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`inherit lldp-app-profile`

Inherit settings from the LLDP Application Type Profile.

`no inherit lldp-app-profile`

Stop inheriting settings from the LLDP Application Type Profile.

lldp app-profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`lldp app-profile <(voice)> diffserv <diffserv>`

Sets the Diffserv value for an LLDP Application Type profile.

lldp app-profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`lldp app-profile <(voice)> priority (low1 | low2 | normal0 | normal3 | high4 | high5 | very-high6 | very-high7)`

Sets the VLAN ID of an LLDP Application Type profile.

lldp app-profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`lldp app-profile <(voice)> tagging (tagged | untagged)`

Sets the VLAN ID of an LLDP Application Type profile.

lldp app-profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`lldp app-profile <(voice)> vlan <vlanid>`

Sets the VLAN Id of an LLDP Application Type profile.

inherit lldp-general

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`inherit lldp-general`

Inherit settings from the LLDP dynamic name.

`no inherit lldp-general`

Inherit settings from the LLDP dynamic name.

lldp dynamic-name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`lldp dynamic-name <name>`

Specifies the text to use for the dynamic name.

You can use regular text in combination with placeholders to create the name. Placeholders are automatically expanded each time the name is regenerated.

Placeholders

%RN	System name of the neighboring device to which the port is connected, obtained via the System Name TLV. Since this is an optional TLV, if it is not available, the Chassis ID TLV is used instead.
%RP	Port description of the port on the neighboring device to which the local port is connected, obtained via the Port Description TLV. Since this is an optional TLV, if it is not available, the Port ID TLV is used instead.

`%SN`	AP's serial number.
`%IP`	AP's IP address. An IP address can require up to 15 characters (nnn.nnn.nnn.nnn).

lldp fast-start-count

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`lldp fast-start-count <count>`

After an MED LLDPDU is received, this timer is started and the agent sends one MED LLDPDU to the MED device each second as it counts down.

lldp holdtime-multiplier

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`lldp holdtime-multiplier <hold>`

Sets the hold time multiplier for LLDPDU transmission.

YThe value of Multiplier is multiplied by the refresh-interval to define Time to live. Time to live indicates the length of time that neighbors will consider LLDP information sent by this agent to be valid.

lldp local-mesh

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`lldp local-mesh`

Enables LLDP support for local mesh links.

`no lldp local-mesh`

Disables LLDP support for local mesh links.

lldp med-location civic-address-element

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`lldp med-location civic-address-element <caelement>`

Adds a Civic Address Element.

lldp med-location elin-addr

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`lldp med-location elin-addr <elin>`

Sets the Emergency Call Services ELIN as described, for example, by NENA TID 07-501.

lldp refresh-interval

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`lldp refresh-interval <time>`

Sets the interval (in seconds) at which local LLDP information is updated and TLVs are sent to neighboring network devices.

lldp run

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`lldp run`

Enables the LLDP Agent on the AP.

`no lldp run`

Disables the LLDP Agent on the AP.

Controlled APs VSC binding context

Path: View > Enable > Controlled APs group > Controlled APs VSC binding

Use this context to configure VSC bindings for controlled APs.

dual radio binding

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dual radio binding (radio1 | radio2)`

Enables radio binding.

`no dual radio binding (radio1 | radio2)`

Disables radio binding.

egress vlan

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`egress vlan`

Enable the egress VLAN.

`no egress vlan`

Disable the egress VLAN.

egress vlan

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`egress vlan <networkname>`

Set the egress vlan.

`no egress vlan`

Disable the egress VLAN.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`end`

Switch to parent context.

location aware

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`location aware <name>`

Set the location-aware group name.

Syslog context

Path: View > Enable > Controlled APs > Controlled APs network configuration > Syslog
View > Enable > Controlled APs group > Controlled APs network configuration > Syslog
View > Enable > Controlled APs base group > Controlled APs network configuration > Syslog

Use this context to define logging options.

message

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`message (matches | notmatches) <regex>`

Use this filter to include log messages. Use a regular expression to define the match criteria for the log file message field.

`no message`

Disables filtering of the log file message field.

message

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`message`

Enables filtering of the log file message field.

`no message`

Disables filtering of the log file message field.

process

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`process (matches | notmatches) <string>`

Use this filter to include log messages according to their process name.

`no process`

Disables filtering of the log file by process name.

process

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`process`

Enables filtering of the log file by process name.

`no process`

Disables filtering of the log file by process name.

level

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`level (lower | higher) (debug | info | notice | warning | error | critical | alert | emergency)`

Defines the severity of messages that will be logged.

`no level`

Disables filtering of the log file by severity level.

Parameters

`debug`	Debug-level messages.
`info`	Informational messages.
`notice`	Normal, but significant condition.
`warning`	Warning conditions.
`error`	Error conditions.
`critical`	Critical conditions.
`alert`	Action must be taken immediately.
`emergency`	System is unusable.

level

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`level`

Enables filtering of the log file by severity level.

`no level`

Disables filtering of the log file by severity level.

matches

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`matches (any | all) filters`

All three log file filters (message, process, and level) are combined to filter the log according to this setting.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`end`

Switch to parent context.

inherit

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`inherit`

Inherit settings from parent.

`no inherit`

Do not inherit setting from parent.

Provisioning connectivity context

Path: View > Enable > Controlled APs > Controlled APs network configuration > Provisioning connectivity
View > Enable > Controlled APs group > Controlled APs network configuration > Provisioning connectivity
View > Enable > Controlled APs base group > Controlled APs network configuration > Provisioning connectivity

Use this context to provision connectivity settings for a controlled AP.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
end
```

Switches to parent context.

inherit

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
inherit
```

Inherit provisioning interface settings from parent.

```
no inherit
```

Do not inherit provisioning interface settings from parent.

interface

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
interface (port1 | local-mesh) (port1 | local-mesh | none)
```

Sets the provisioning interface.

interface provisioning

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
interface provisioning
```

Enables interface provisioning.

```
no interface provisioning
```

Disables interface provisioning.

ip assignation

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
ip assignation (static | dhcp)
```

Sets the IP assignment method.

vlan

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`vlan`

Enables use of the provisioning VLAN.

`no vlan`

Disables use of the provisioning VLAN.

vlan

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`vlan <id>`

Sets the provisioning VLAN.

`no vlan`

Disables use of the provisioning VLAN.

static ip

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`static ip <ip> <netmask> <gateway>`

Sets the static IP address.

provisioning local mesh group

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`provisioning local mesh group <id>`

Sets the local mesh ID.

provisioning local mesh key

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`provisioning local mesh key <key>`

Sets the local mesh security key.

provisioning local mesh port

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`provisioning local mesh port (radio1 | radio2)`

Sets the radio used for local mesh.

provisioning local mesh security

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`provisioning local mesh security`

Enables the use of local mesh security.

`no provisioning local mesh security`

Disables the use of local mesh security.

provisioning local mesh security

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`provisioning local mesh security (wep | tkip | ccmp)`

Sets the local mesh security mode.

`no provisioning local mesh security`

Disables the use of local mesh security.

provisioning local mesh type

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`provisioning local mesh type (a | b | g | bg)`

Sets the wireless mode for local mesh.

country code

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`country code <code>`

Sets the country code for local mesh.

anonymous identity

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`anonymous identity <identity>`

Changes the anonymous identity.

eap

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`eap (peap0 | peap1 | ttls) <user> <password>`

Changes the EAP configuration.

ieee8021x provisioning

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ieee8021x provisioning`

Enables IEEE 802.1X provisioning.

`no ieee8021x provisioning`

Disables IEEE 802.1X provisioning.

Provisioning discovery context

Path: View > Enable > Controlled APs > Controlled APs network configuration > Provisioning discovery
View > Enable > Controlled APs group > Controlled APs network configuration > Provisioning discovery
View > Enable > Controlled APs base group > Controlled APs network configuration > Provisioning discovery

Use this context to provision discovery settings for a controlled AP.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`end`

Switches to parent context.

dns name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dns name <name>`

Adds a DNS name to the list.

`no dns name <name>`

Deletes a DNS name from the list.

dns provisioning

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dns provisioning`

Enables DNS provisioning.

`no dns provisioning`

Disables DNS provisioning.

inherit

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`inherit`

Inherit provisioning discovery settings from parent.

`no inherit`

Do not inherit provisioning discovery settings from parent.

dns domain name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dns domain name <name>`

Sets the DNS domain name.

dns server

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dns server <ip>`

Adds a DNS server to the list.

`no dns server <ip>`

Deletes a DNS server from the list.

discovery provisioning

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`discovery provisioning`

Enables discovery provisioning.

`no discovery provisioning`

Disables discovery provisioning.

ip address

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ip address <ip>`

Adds an IP address to the list.

`no ip address <ip>`

Deletes an IP address from the list.

ip provisioning

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ip provisioning`

Enables IP provisioning.

`no ip provisioning`

Disables IP provisioning.

Wireless interface context

Path: View > Enable > Controlled APs > Controlled APs network configuration > Wireless interface
View > Enable > Controlled APs group > Controlled APs network configuration > Wireless interface
View > Enable > Controlled APs base group > Controlled APs network configuration > Wireless interface

Use this context to configure wireless settings.

dot11

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dot11 <mode> <frequency>`

Sets the wireless mode and the frequency the controller will operate at.

Parameters

<mode>	Sets the transmission speed and frequency band. The available options are determined by the wireless card installed in the controller, and may include: a: Selects 802.11a providing 54 Mbps in the 5 GHz frequency band. b: Selects 802.11b providing 11 Mbps in the 2.4 GHz frequency band. g: Selects 802.11g providing 54 Mbps in the 2.4 GHz frequency band. bg: Selects 802.11b + 802.11g providing 11 and 54 Mbps in the 2.4 GHz frequency band. n: Selects 802.11n. an: Selects 802.11n + 802.11a, on the 5Ghz frequency band. gn: Selects 802.11n + 802.11g, on the 2.4Ghz frequency band. bgn: Selects 802.11n + 802.11g + 802.11b, on the 2.4Ghz frequency band.
<frequency>	Sets the operating frequency by specifying a number in GHz or by specifying a channel number. The frequencies that are available are determined by the radio installed in the controller and the regulations that apply in your country. For optimum performance when operating in 802.11b or 802.11g modes, choose a frequency that differs from other wireless access points operating in neighboring cells by at least 25 MHz. If operating in 802.11a mode, all channels are non-overlapping.

distance

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`distance (small | medium | large)`

Sets the distance between access points.

Use this parameter to adjust the receiver sensitivity of the controller. This parameter should only be changed if:

- you have more than one wireless access point installed in your location
- you are experiencing throughput problems

In all other cases, use the default setting of Large.

If you have installed multiple controllers, reducing the receiver sensitivity of the controller from its maximum will help to reduce the amount of crosstalk between the wireless stations to better support roaming clients. By reducing the receiver sensitivity, client stations will be more likely to connect with the nearest access point.

transmit power

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`transmit power (DB | max)`

Sets the maximum transmission power of the wireless radio.

Parameters

<db> Power is specified in steps of 1dBm. The maximum setting is 18 dBm.

Note: The actual transmit power used may less than the value specified. The controller determines the power to used based on the settings you made for regulatory domain, wireless mode, and operating frequency.

multicast rate

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`multicast rate (1 | 2 | 5.5 | 6 | 9 | 11 | 12 | 18 | 24 | 36 | 48 | 54)`

Sets the transmit rate for multicast traffic.

This is a fixed rate, which means that if a station is too far away to receive traffic at this rate, then the multicast will not be seen by the station. By rasing the multicast rate you can increase overall throughput significantly.

dot11 automatic frequency

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dot11 automatic frequency`

Enable this option to have the controller automatically determine the best operating frequency.

`no dot11 automatic frequency`

Disable automatic frequency selection.

dot11 automatic frequency period

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dot11 automatic frequency period (disabled | 1h | 2h | 4h | 8h | 12h | 24h)`

Specify how often the frequency setting is re-evaluated when automatic frequency selection is enabled.

dot11 automatic frequency time

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dot11 automatic frequency time <time>`

Specify when the channel should be re-evaluated.

dot11 automatic transmit-power

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
dot11 automatic transmit-power
```

Enables automatic transmit power selection.

```
no dot11 automatic transmit-power
```

Disables automatic transmit power selection.

dot11 automatic transmit-power period

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
dot11 automatic transmit-power period (1h | 2h | 4h | 8h | 12h | 24h)
```

Sets the interval at which the transmit power setting is re-evaluated when automatic power selection is enabled.

antenna bidirectionnal

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
antenna bidirectionnal (diversity | main | auxiliary)
```

Sets the antenna to transmit and receive on. Select diversity to transmit and receive on both antennas.

Parameters

`diversity`	In this mode both antennas are used to transmit and receive. The controller supports both transmit and receive diversity.
`main`	Transmit and receive on the main antenna only.
`aux`	Transmit and receive on the aux antenna only.

antenna gain

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
antenna gain <number>
```

Used only for Radar detection, records gain (in 5GHz band) of external antenna installed on device. Does not affect output power.

autochannel skip

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
autochannel skip <chan>
```

Adds the specified channel to the list of channels that are not allowed to be selected by the Auto Channel algorithm.

station distance

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
station distance (0km | 5km | 10km | 15km | 20km | 25km | 30km | 35km)
```

Fine tunes internal timeout settings to account for the distance that wireless links span. For normal operation, the controller is optimized for links of less than 1 km.

This is a global setting that is useful when creating wireless links to remote sites. However, it also applies to all wireless connection made with the radio, not just for wireless links. Therefore, if you are also using the radio to serve local wireless client stations, adjusting this setting may lower the performance for clients with marginal signal strength or when interference is present.
(Essentially, it means that if a frame needs to be retransmitted it will take longer before the actual retransmit takes place.)

beacon interval

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`beacon interval <value>`

Sets the beacon interval.

Parameters

`< value>`	Beacon interval value in the range 20 and 500 time units (TU) (1 TU = 1024us).

rts threshold

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`rts threshold <value>`

Sets the RTS threshold.

`no rts threshold`

Deletes the RTS threshold value.

Parameters

`< value>`	Threshold value in the range 128 and 1540.

Description

Use this parameter to control collisions on the link that can reduce throughput. If the Status > Wireless page on the management tool shows increasing values for Tx multiple retry frames or Tx single retry frames, you should adjust this value until the errors clear up. Start with a value of 1024 and then decrease to 512 until errors are reduced or eliminated.

Using a small value for RTS threshold can affect throughput.

If a packet is larger than the threshold, the controller will hold it and issue a request to send (RTS) message to the client station. Only when the client station replies with a clear to send (CTS) message will the controller send the packet. Packets smaller than the threshold are transmitted without this handshake.

dot11 mode

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dot11 mode (monitor | ap+wds | ap-only | wds-only | sensor)`

Sets the operating mode for the radio.

radio active

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radio active`

Enables the radio.

```
no radio active
```

Disables the radio.

spectralink view

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
spectralink view
```

Enables the use of spectralink view.

```
no spectralink view
```

Disables the use of spectralink view.

New

client statistics

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
client statistics
```

Enable collect statistics for wireless clients.

```
no client statistics
```

Disable collect statistics for wireless clients.

dot11n guard interval

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
dot11n guard interval (short | long)
```

Selects the 802.11n guard interval.

dot11n mimo

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
dot11n mimo (3x3 | 2x2 | 2x3)
```

Sets the MIMO mode for 802.11n.

dot11n channel width

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
dot11n channel width (40 | 20 | auto)
```

Select the 802.11n channel width.

dot11n channel extension

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
dot11n channel extension (above | below)
```

Selects the 802.11n channel extension. Applicable only in the 2.4 GHz band and a 40 MHz channel width.

dot11n mac protection

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
dot11n mac protection (none | cts-to-self | rts-cts)
```

Sets the RTS/CTS protection mode for 802.11n.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
end
```

Switches to parent context.

inherit

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
inherit
```

Inherit settings from parent.

```
no inherit
```

Do not inherit settings from parent.

RADIUS profile context

Path: View > Enable > Controlled APs > Controlled APs network configuration > RADIUS profile
View > Enable > Controlled APs group > Controlled APs network configuration > RADIUS profile
View > Enable > Controlled APs base group > Controlled APs network configuration > RADIUS profile

Use this context to define basic settings for RADIUS profiles.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
end
```

Switch to parent context.

inherit

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
inherit
```

Inherit settings from parent.

```
no inherit
```

Do not inherit settings from parent.

radius nas id

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
radius nas id <nasid>
```

Sets the RADIUS profile NAS Id.

Local mesh profile context

Path: View > Enable > Controlled APs > Controlled APs network configuration > Local mesh profile
View > Enable > Controlled APs group > Controlled APs network configuration > Local mesh profile
View > Enable > Controlled APs base group > Controlled APs network configuration > Local mesh profile

Use this context to define settings for local mesh profiles.

security

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
security
```

Enables wireless security.

```
no security
```

Disables wireless security.

security mode

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
security mode (wep | tkip | ccmp)
```

Set the security mode.

security psk

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
security psk <secret>
```

Sets the PSK secret.

```
no security psk
```

Clears the PSK secret.

security wep

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
security wep <key>
```

Sets the WEP key.

```
no security wep
```

Deletes the WEP key.

dynamic mode

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
dynamic mode(master|alt-master|slave)
```

Selects the mode of operation for dynamic mode.

Three different roles can be assigned to a local mesh node: master, alternate master, or slave. Each role governs how upstream and downstream links are established by the node.

Parameters

<master>	Root node that provides the upstream link to the root network that the other nodes want to reach. The master never tries to connect to any other node. It waits for links from downstream alternate master or slave nodes. .
<alt-master>	First establishes an upstream link with a master or alternate master node. Next, operates as a master node waits for links from downstream alternate master or slave nodes.
<slave>	Can only establish an upstream link with master or alternate master node. Slave nodes cannot establish downstream links with other nodes.

mesh id

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`mesh id <id>`

Sets the mesh ID.

allowed downtime

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`allowed downtime <number>`

The maximum time (in seconds) that a link can remain idle before the link actually gets deleted. When a slave (or alternate-master) loses its link to its master, the discovery phase is re-initiated.

minimum snr

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`minimum snr <number>`

(Alternate Master, Slave only) This node will only connect with other nodes whose SNR is above this setting (in dB).

snr cost per hop

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`snr cost per hop <number>`

(Alternate Master, Slave only) This value is an estimate of the cost of a hop in terms of SNR. It indicates how much SNR a node is willing to sacrifice in order to connect to node one hop closer to the root node, because each hop has an impact on performance, especially when using a single radio.)

initial discovery time

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`initial discovery time <number>`

(Alternate Master, Slave only) Amount of time that will be taken to discover the best available master node.

The goal of this setting is to delay discovery until all the nodes in the surrounding area have had time to startup, making the identification of the best master more accurate. If this period is too short, a slave may connect to the first master it finds, not necessarily the best.

active

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`active`

Activates the local mesh profile.

`no active`

Deactivates the local mesh profile.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`end`

Switch to parent context.

inherit

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`inherit`

Inherit settings from parent.

`no inherit`

Do not inherit settings from parent.

name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`name <name>`

Renames the current local mesh group.

radio active

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`radio active (radio1 | radio2)`

Enables the radio.

`no radio active (radio1 | radio2)`

Disables the radio.

Local mesh provisioning context

Path: View > Enable > Controlled APs > Controlled APs network configuration > Local mesh provisioning
View > Enable > Controlled APs group > Controlled APs network configuration > Local mesh provisioning
View > Enable > Controlled APs base group > Controlled APs network configuration > Local mesh provisioning

Use this context to define configuration settings for the local mesh provisioning profile on a controlled AP.

accept connection

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
accept connection
```

Sets the local mesh provisioning profile to act as an alternate master.

```
no accept connection
```

Prevents the local mesh provisioning profile from acting as an alternate master.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
end
```

Switches to parent context.

inherit

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
inherit
```

Inherit settings from parent.

```
no inherit
```

Do not inherit settings from parent.

multiple radio

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
multiple radio
```

On multiple radio products, use all available radios.

```
no multiple radio
```

On multiple radio products, do not use all available radios.

Switch port context

Path: View > Enable > Controlled APs > Controlled APs network configuration > Switch port
View > Enable > Controlled APs group > Controlled APs network configuration > Switch port
View > Enable > Controlled APs base group > Controlled APs network configuration > Switch port

Use this context to define settings for a switch port.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
end
```

Back to parent context.

active

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
active
```

Activates this port.

```
no active
```

Deactivates this port.

app-profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
app-profile
```

Enables a LLDP MED application type profile on this port.

```
no app-profile
```

Disables an LLDP MED application type profile on this port.

app-profile

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
app-profile <(voice)>
```

Sets an LLDP MED application type profile on this port.

```
no app-profile
```

Disables an LLDP MED application type profile on this port.

authentication profile vsc

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
authentication profile vsc <name>
```

Sets the VSC (Virtual AP) to use for authentication.

```
use authentication profile vsc
```

Use the VSC (Virtual AP) for authentication.

`no use authentication profile vsc`

Ignore the VSC (Virtual AP) for authentication.

authentication server radius

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`authentication server radius <name>`

Selects the RADIUS profile to use.

dot1x authentication

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dot1x authentication`

Enables support for IEEE802.1X.

`no dot1x authentication`

Disables support for IEEE802.1X.

dynamic vlan

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dynamic vlan`

Enables dynamic VLAN.

`no dynamic vlan`

Disables dynamic VLAN.

egress rate

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`egress rate <(128k|256k|512k|1m|2m|4m|8m|16m|32m)>`

Sets the maximum rate at which this port will accept egress traffic.

`use egress rate`

Limit the egress data rate.

`no use egress rate`

Do not limit the egress data rate.

force flow control

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`force flow control`

Forces flow control on this port.

`no force flow control`

Do not force flow control on this port.

ingress rate

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ingress rate <(128k|256k|512k|1m|2m|4m|8m|16m|32m)>`

Set the maximum rate at which this port will accept ingress traffic.

`use ingress rate`

Limit the ingress data rate.

`no use ingress rate`

Do not limit the ingress data rate.

ingress traffic type

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ingress traffic type (broadcast | multicast+broadcast | all)`

Select the type of traffic to which rate limiting applies.

loop protection

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`loop protection`

Enables loop protection on this port.

`no loop protection`

Disables loop protection on this port.

mac authentication

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`mac authentication`

Enables support for MAC-based authentication.

`no mac authentication`

Disables support for MAC-based authentication.

mac filter list

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`mac filter list <name>`

Accept the MAC addresses defined in the specified list.

`no mac filter list <name>`

Remove this list of MAC ranges.

poe-class-support

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`poe-class-support (class1-2 | class0-3)`

Set the Power over Ethernet limit.

Parameters

`class1-2`	Provide power to devices conforming to 802.11af class 1 and class 2.
`class0-3`	Provide power to devices conforming to 802.11af class 0, 1, 2 and 3.

port name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`port name <name>`

Changes the port name.

port type

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`port type (tagged | untagged)`

Configure the port type.

power over ethernet

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`power over ethernet`

Enables PoE on this port.

`no power over ethernet`

Disables PoE on this port.

priority

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`priority (low | medium | high | very-high)`

Sets the default QoS priority for this port.

priority lookup

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`priority lookup (diffsrv | 802.1p | any)`

Chooses the port priority lookup.

`use priority lookup`

Turns on priority lookup for this port.

`no use priority lookup`

Turns on priority lookup for this port.

quarantine vlan

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`quarantine vlan <number>`

Sets the quarantine VLAN ID.

`no quarantine vlan`

Clears the quarantine VLAN.

`use quarantine vlan`

Enables the quarantine VLAN setting.

`no use quarantine vlan`

Disables the quarantine VLAN setting.

secondary vlan

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`secondary vlan <number>`

Sets the secondary VLAN ID.

`no secondary vlan`

Clears the secondary VLAN ID.

`use secondary vlan`

Enables the secondary VLAN setting.

`no use secondary vlan`

Disables the secondary VLAN setting.

vlan

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`vlan <number>`

Sets the VLAN ID for this port.

`use vlan`

Applies the VLAN.

`no use vlan`

Disables the VLAN.

MAC addresses list context

Path: View > Enable > Config > MAC addresses list

Use this context to manage the MAC address lists. Each list can contain the MAC addresses of one or more devices. The lists can be assigned to the MAC filter option on a switch port, permitting you to limit switch port access to a specific devices based on their MAC address.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`end`

Go to previous context.

entry

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`entry <mac>`

Adds a new entry with the specified MAC address to the list.

`no entry <mac>`

Removes the entry with the specified MAC address from the list.

list name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`list name <string>`

Changes the current list name.

Network profile context

Path: View > Enable > Config > Network profile

Use this context to configure network profiles.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
end
```

Go to previous context.

name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
name <string>
```

Changes the name of current network profile.

vlan

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
vlan
```

Enables a VLAN ID for this network profile.

```
no vlan
```

Disables the VLAN ID for this network profile.

vlan

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
vlan <number>
```

Sets the VLAN ID for this network profile.

```
no vlan
```

Disables the VLAN ID for this network profile.

New

default

Supported on: E-MSM720

```
default
```

Selects the current VLAN ID as the default VLAN.

LLDP agent context

Path: View > Enable > Config > LLDP agent

Use this context to configure LLDP settings for controllers and APs.

admin-status

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
admin-status (tx_rx | txonly | rxonly | disable)
```

Enables LLDP agent functionality on this port.

basic-tlv-enable

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
basic-tlv-enable
```

Enables support for basic TLVs.

```
no basic-tlv-enable
```

Disables support for basic TLVs.

basic-tlv-enable port_desc

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
basic-tlv-enable port_desc
```

Enables the port description TLV.

```
no basic-tlv-enable port_desc
```

Disables the port description TLV.

basic-tlv-enable system_cap

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
basic-tlv-enable system_cap
```

Enables the system capabilities TLV.

```
no basic-tlv-enable system_cap
```

Disables the system capabilities TLV.

basic-tlv-enable system_descr

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
basic-tlv-enable system_descr
```

Enables the system description TLV.

```
no basic-tlv-enable system_descr
```

Disables the system description TLV.

basic-tlv-enable system_name

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`basic-tlv-enable system_name`

Enables the system name TLV.

`no basic-tlv-enable system_name`

Disables the system name TLV.

dot3-tlv-enable

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`dot3-tlv-enable`

Enables the 803.3 MAC/PHY TLV.

`no dot3-tlv-enable`

Disables the 803.3 MAC/PHY TLV.

end

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`end`

Go to previous context.

ip-addr-enable

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`ip-addr-enable <ipaddress>`

Sets the IP address to be enabled.

med-application-type

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`med-application-type <type>`

Sets MED Application Type for this port.

medtlv-enable capabilities

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

`medtlv-enable capabilities`

Enables the MED Capabilities TLV.

`no medtlv-enable capabilities`

Disables the MED Capabilities TLV.

medtlv-enable location-id

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
medtlv-enable location-id
```

Enables the MED Location TLV.

```
no medtlv-enable location-id
```

Disables the MED Location TLV.

medtlv-enable network-policy

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
medtlv-enable network-policy
```

Enables the MED Network Policy TLV.

```
no medtlv-enable network-policy
```

Disables the MED Network Policy TLV.

medtlv-enable poe

Supported on: MSM710 E-MSM720 MSM760 MSM765zl

```
medtlv-enable poe
```

Enables the MED Power-via-MDI TLV.

```
no medtlv-enable poe
```

Disables the MED Power-via-MDI TLV.

Technology for better business outcomes

To learn more, visit www.hp.com/networking/

© Copyright 2011 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP will not be liable for technical or editorial errors or omissions contained herein.

December 2011

Manual Part Number
5998-1432